

**POLÍTICA DE PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA DA PUMA
COORDENADORA DE OFERTAS PÚBLICAS LTDA.**

SUMÁRIO

1.	OBJETIVO.....	3
2.	PREMISSAS.....	5
3.	MECANISMOS DE PROTEÇÃO E PREVENÇÃO.....	11
4.	PROTEÇÃO E TRATAMENTO DE DADOS PESSOAIS.....	18
5.	DISPOSIÇÕES GERAIS.....	19
6.	HISTÓRICO DAS ATUALIZAÇÕES DA POLÍTICA DE SIGILO DE INFORMAÇÕES.....	19
	ANEXO I.....	20

1. OBJETIVO

1.1. Introdução

Esta Política de Proteção de Dados e Segurança Cibernética ("**Política de Sigilo de Informações**") da Puma Coordenadora de Ofertas Públicas Ltda., inscrita no CNPJ sob o nº 67.219.697/0001-67 ("**Puma**" ou "**Coordenadora**"), é elaborada em conformidade com o disposto na Resolução da Comissão de Valores Mobiliários ("**CVM**") nº 161, de 13 de julho de 2022, conforme alterada ("**Resolução CVM nº 161**"), e demais orientações da CVM e da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("**Anbima**"), tendo por objetivo dispor sobre regras e procedimentos que assegurem a confidencialidade, o sigilo e a integridade dos dados, informações e sistemas computacionais utilizados pela Puma.

A Coordenadora atua prezando pela total transparência e respeito às leis e normas, aos participantes do mercado financeiro e de capitais e seus clientes, sendo certo que esta Política de Sigilo de Informações reúne as diretrizes obrigatórias, vinculantes e inderrogáveis que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando o atendimento de regulatórios.

Nesta Política de Sigilo de Informações incorpora-se assuntos relacionados à captação, controle, gerenciamento e destruição de informações de clientes, prestadores e demais contrapartes em operações.

A Política de Sigilo de Informações deverá ser revisada, no mínimo, anualmente, considerando, entre outros fatores, alterações na legislação e regulamentação aplicáveis, bem como eventuais deficiências identificadas em sua implementação. Adicionalmente, esta Política de Sigilo de Informações poderá ser atualizada a qualquer tempo, sempre que a Diretora de Compliance e PLD/FTP ou a Alta Administração (abaixo definidos) assim entenderem necessário, visando garantir sua efetividade e aderência ao perfil de risco da Coordenadora.

A Coordenadora deverá preparar e manter versões atualizadas desta Política de Sigilo de Informações em seu website, juntamente com os seguintes documentos ("**Políticas**"): (i) o Código de Ética; (ii) a Política de Compliance e Controles Internos; (iii) a Política de Suitability; (iv) a Política de Investimentos Pessoais; e (v) a Política de PLD/FTP. Eventuais termos iniciados em letras maiúsculas e não definidos nesta Política de Sigilo de Informações deverão ter o significado atribuído nas demais Políticas.

1.1. Responsabilidades

A coordenação direta das atividades relacionadas a esta Política de Sigilo de Informações é uma atribuição da Diretora de Compliance e PLD/FTP, diretora estatutária da Coordenadora, nos termos da Resolução CVM nº 161, conforme indicado no Formulário de Referência da Coordenadora. A Diretora de Compliance e PLD/FTP reporta-se somente à **“Alta Administração”** da Coordenadora, composta por seus diretores estatutários, sendo sua atuação pautada na autonomia e independência.

A Diretora de Compliance e PLD/FTP poderá ser auxiliada por Colaboradores integrantes da **“Equipe de Compliance”**, devidamente treinados, atualizados e com conhecimento compatível com as respectivas funções desempenhadas (**“Área de Compliance”**).

1.2. Aplicabilidade da Política de Sigilo de Informações

Esta Política de Sigilo de Informações aplica-se a todos os Colaboradores da Puma, em especial aqueles que, por meio de suas relações ou funções junto à empresa, podem ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, regulatória, negocial, econômica, dentre outras.

1.3. Termo de Confidencialidade

Esta Política de Sigilo de Informações é parte integrante das políticas internas da Coordenadora, em especial das sociedades que se constituem como coordenadoras de ofertas públicas de valores mobiliários, sendo que todos os Colaboradores após o recebimento desta Política de Sigilo de Informações firmarão o termo de recebimento e compromisso constante do **“Anexo I”** a esta Política de Sigilo de Informações (**“Termo de Confidencialidade”**), reconhecendo e confirmando seu entendimento e concordância com o aqui disposto e com as demais diretrizes, normas, princípios, conceitos e valores da Coordenadora, comprometendo-se, ainda, a zelar pela aplicação das normas de sigilo e confidencialidade aqui descritas, bem como nas demais Políticas.

Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos desta Política de Sigilo de Informações e demais Políticas.

1.4. Sanções

Suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos nesta Política de Sigilo de Informações ou das demais normas aplicáveis às atividades da Coordenadora deverão ser levados para apreciação da Diretora de Compliance e PLD/FTP de acordo com os procedimentos estabelecidos.

Ressalta-se que é dever de todo Colaborador informar à Área de Compliance sobre quaisquer violações ou possíveis violações dos princípios e normas aqui dispostos. Caso a violação ou suspeita de violação recaia sobre a própria Diretora de Compliance e PLD/FTP, o Colaborador deverá informar diretamente a Alta Administração.

Competirá à Diretora de Compliance e PLD/FTP definir e aplicar as sanções decorrentes de tais desvios, nos termos desta Política de Sigilo de Informações, respeitando o contraditório. Caso a conduta avaliada seja imputada à própria Diretora de Compliance e PLD/FTP, a definição e aplicação da sanção ficará a cargo da Alta Administração.

As sanções aplicáveis são: (i) advertência; (ii) suspensão; (iii) desligamento ou exclusão por justa causa; e (iv) demissão por justa causa.

Não obstante a aplicação das sanções, a Coordenadora poderá ainda pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis, bem como não assumirá responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções, podendo, inclusive, exercer o direito de regresso em face dos responsáveis, caso venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores.

2. PREMISSAS

2.1. Definições

(i) **“Informação Confidencial”**: significa quaisquer informações reservadas ou privilegiadas sobre a Puma, sua atividade de coordenação, seus Colaboradores, clientes, prestadores de serviços e demais contrapartes (a) que não seriam normalmente obtidas por meio do acesso regular à rede mundial de computadores ou à diretórios de dados públicos, independentemente de estarem contidas em meios físicos ou digitais, e (b) que foram obtidas em razão de uma relação especial de confiança e prestação de serviço pela Puma, individual ou coletiva, direta ou indiretamente, incluindo, exemplificadamente:

- a) Informações pessoais de Colaboradores da Puma, de clientes, prestadores de serviços e demais contrapartes, tais como endereços, nomes, números cadastrais, informações financeiras e mais;
- b) Quaisquer informações envolvendo decisões de acionista controlador, deliberações de assembleia geral ou de órgãos de administração, bem como atos ou fatos de caráter político-administrativo, técnico, negocial ou econômico-financeiro relativos aos negócios da Puma ou de clientes, que

possam ou não influir na cotação de valores mobiliários, na decisão de investidores de negociar tais ativos ou de exercer direitos a eles inerentes;

c) Informações sobre resultados financeiros, balanços, balancetes e demonstrações financeiras da Coordenadora ou de clientes, antes de sua efetiva publicação e divulgação oficial ao mercado;

d) Operações, negócios, parcerias ou transações financeiras e societárias realizadas ou em fase de negociação que ainda não tenham sido divulgadas publicamente;

e) Estruturas organizacionais, planos de ação, metas de negócios, relações e listagens de clientes, contrapartes comerciais, investidores prospectados, fornecedores e prestadores de serviços;

f) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e comerciais, incluindo saldos, extratos, movimentações, carteiras e posições de investimento de clientes;

g) *Know-how*, metodologias de análise, técnicas de estruturação, cópias, diagramas, modelos de precificação, amostras, códigos-fonte e programas de computador proprietários ou customizados;

h) Quaisquer dados, comunicações ou informações obtidas junto a sócios, diretores, colaboradores, estagiários e jovens aprendizes ou junto a seus assessores e consultores da Puma, que não tenham sido expressamente autorizadas para divulgação pública;

i) Informações sobre o processo de sondagem de mercado (*market sounding*), *pilot fishing*, ordens de reserva, demandas, volumes, taxas de corte e intenções de investimento coletadas junto a investidores institucionais ou qualificados antes da precificação oficial da oferta;

j) Quaisquer relatórios, questionários, auditorias jurídicas, financeiras ou socioambientais (ESG) e minutas de documentos da oferta (*prospectos*, lâminas, contratos de coordenação) gerados durante a fase de auditoria e estruturação de emissão e oferta; e

k) Ofícios, cartas, exigências, consultas formais ou informais e respostas trocadas com a CVM, Anbima, B3 ou outras entidades administradoras de mercado organizado, cujo teor ou existência ainda não sejam públicos.

(ii) “**Risco Cibernético**”: significa a probabilidade de ocorrência de qualquer evento, falha ou ataque em ambientes digitais utilizados pela Coordenadora que resulte em vazamento de Informações Confidenciais, perda de dados, prejuízos financeiros ou prejuízos à reputação da Puma, seus Colaboradores, clientes, prestadores de serviços e demais contrapartes. São consideradas práticas que constituem risco cibernético às atividades de coordenação da Puma, sem prejuízo de outras:

a) Ransomware (Sequestro de Dados): Software malicioso que criptografa sistemas e bancos de dados da instituição, interrompendo as operações e exigindo o pagamento de resgate para a liberação da chave de acesso;

b) Trojans: Programas maliciosos camuflados como arquivos ou softwares legítimos que, ao serem executados por colaboradores, criam portas de acesso ocultas para invasores na rede interna;

c) Spywares e Vírus: Aplicações infiltradas nas estações de trabalho com o objetivo de monitorar atividades, roubar credenciais de acesso (*keyloggers*) ou corromper a integridade de arquivos e sistemas operacionais;

d) Phishing, Smishing e Vishing: Vetores de indução ao erro nos quais fraudadores disparam comunicações eletrônicas (e-mails, SMS) ou realizam chamadas telefônicas simulando marcas ou executivos de confiança para capturar dados confidenciais ou credenciais de funcionários;

e) Pharming (Envenenamento de DNS): Ataque que corrompe o direcionamento de tráfego da internet, fazendo com que o colaborador acesse um site falso (idêntico ao sistema interno ou bancário legítimo) mesmo digitando o endereço correto no navegador;

f) Espionagem Visual (Shoulder Surfing): Captação não autorizada de dados confidenciais por terceiros mediante a observação direta de telas de notebooks ou celulares de colaboradores que estejam trabalhando em ambientes públicos ou regimes de *home office*;

g) Negação de Serviço Distribuída (DDoS) via Botnets: Ataques coordenados por redes de computadores zumbis (*botnets*) que inundam os servidores da instituição com tráfego massivo, visando indisponibilizar sistemas internos, plataformas de clientes ou portais de ofertas;

h) Ameaças Avançadas e Persistentes (APTs): Campanhas de intrusão cibernética altamente sofisticadas e direcionadas, conduzidas por agentes que buscam se manter infiltrados e invisíveis na rede corporativa por longos períodos para exfiltrar dados estratégicos de forma contínua;

i) Ataques à Cadeia de Suprimentos (Supply Chain Attack): Comprometedores de segurança que ocorrem através de vulnerabilidades em softwares ou sistemas de fornecedores estratégicos terceirizados (ex.: plataformas de *bookbuilding*, auditorias ou serviços de nuvem);

j) Shadow IT e Inteligência Artificial: Uso de Sistemas Não Homologados (conforme definido abaixo) por esta Política de Sigilo de Informações e o envio de minutas e documentos da Puma, seus clientes, prestadores de serviço e demais contrapartes de prospectos ou relatórios financeiros confidenciais para ferramentas públicas de Inteligência Artificial para revisão de texto, expondo dados sigilosos na nuvem pública;

k) Comprometedores de E-mail Corporativo (Ataque BEC - Business Email Compromise): Invasão ou clonagem perfeita da conta de e-mail de um diretor ou parceiro estratégico, utilizada para enviar instruções fraudulentas de transferências bancárias, liquidações ou alteração de dados de contas de destino para investidores; e

l) Sequestro e Abuso de APIs (API Hijacking): Exploração de brechas de segurança nas interfaces de programação de aplicativos (APIs) que conectam os sistemas da coordenadora a parceiros, custodiantes, bancos de liquidação ou à própria CVM/B3, permitindo o desvio de dados em trânsito.

(iii) **“Sistemas Não Homologados”**: significa quaisquer aplicações, endereços eletrônicos, sistemas informacionais, redes sociais, aplicativos de mensagens e correio eletrônico e inteligências artificiais, dentre outros, cujo uso profissional não tenha sido expressamente recomendado pela Alta Administração da Coordenadora; e

(iv) **“Colaborador”**: significa, individual ou coletivamente, todos os empregados da Coordenadora, funcionários terceirizados, diretores estatutários, com ou sem função regulatória específica definida no ato constitutivo e sócios da Puma.

2.2. Princípios

Cada Colaborador da Coordenadora, de forma inderrogável vinculado a esta Política de Sigilo de Informações, deve adotar o mais elevado grau de fidúcia para com a Puma e

seus clientes quando da obtenção, posse, manuseio, envio, compartilhamento e destruição de documentos contendo Informações Confidenciais, garantindo a observação dos seguintes princípios:

- (i) Confidencialidade. Restrição de Informações Confidenciais estritamente aos titulares e a usuários previamente autorizados pela Alta Administração, sejam Colaboradores da Puma, clientes ou prestadores de serviços, somente na medida necessária para o desenvolvimento da atividade de coordenação da Coordenadora;
- (ii) Integridade e Qualidade dos Dados. Preservação integral, sem modificação ou destruição acidentais ou não autorizadas pela Alta Administração, do conteúdo dos documentos recebidos no desenvolvimento das atividades de coordenação da Coordenadora, exceto quando previamente autorizado;
- (iii) Disponibilidade. Acesso contínuo e oportuno às Informações Confidenciais sempre que necessário para a condução das operações, assegurando que tais dados fiquem salvaguardados aos titulares e às autoridades competentes em ambiente seguro pelo prazo de guarda, sendo terminantemente vedada a sua destruição precoce;
- (iv) Rastreabilidade. Registro completo e integral da cadeia de origem, modificação e envio de quaisquer Informações Confidenciais em posse da Coordenadora, de forma que todo o seu ciclo de vida (quem acessou, quem enviou e quem modificou) seja devidamente registrado em trilhas de auditoria inalteráveis, permitindo a prestação de contas (*accountability*) perante os órgãos reguladores; e
- (v) Prevenção. Implemento de medidas de segurança preventivas, visando evitar o vazamento de quaisquer Informações Confidenciais e mitigar Riscos Cibernéticos quando da coleta, manuseio e compartilhamento de Informações Confidenciais, através de testes de controle e outras medidas previstas abaixo.

2.3. Conflitos de Interesse

Situações de conflitos de interesses ocorrem quando as atividades desempenhadas pela Puma ou pelos seus Colaboradores sejam conflitantes com seus próprios interesses pessoais, interesses da Puma e/ou interesses dos clientes emissores ou investidores das ofertas públicas as quais forem coordenadas pela Puma.

Em observância à correta e adequada transparência regulatória e informacional, a Puma, desde já, esclarece que integra grupo econômico no qual atua a Patagônia

Capital Gestora de Recursos Ltda., inscrita sob o CNPJ nº 39.526.263/0001-74 (“**Patagônia Capital**” ou “**Gestora**”), sobre controle comum dos Sócios da Puma.

Especialmente para os fins desta Política de Sigilo de Informações, não serão compartilhados o mesmo espaço físico (as atividades se darão em salas diferentes), diretórios de arquivos (existirão usuários e *drives* separados) e sistemas de informação (diretório de arquivos, correio eletrônico, aplicativos de mensagens corporativa, edição e elaboração de documentos) entre a Coordenadora e a Gestora, a fim de evitar que Informações Confidenciais da Puma e seus clientes transitem entre o diretório de arquivos, sistemas de informação e recursos computacionais da Gestora, exceto quanto previamente autorizado pela Alta Administração e/ou necessário em virtude de uma coordenação de oferta específica em que a Gestora participe junto à Coordenadora, respeitando a autonomia funcional.

Nesse sentido, de forma complementar, a Puma se compromete a adotar as seguintes medidas para identificar possíveis conflitos de interesses, observando a boa-fé e o dever de diligência em suas atividades, incluindo, mas não se limitando, a:

- (i) monitoramento de canais de comunicação dos Colaboradores da Puma;
- (ii) realização de treinamentos em cibersegurança aos Colaboradores da Puma; e
- (iii) monitoramento contínuo das atividades potencialmente conflitantes em operações compartilhadas entre Gestora e Coordenadora.

Na ocorrência de um caso concreto em que seja vislumbrada uma situação de conflito de interesses, os Colaboradores envolvidos devem, imediatamente, comunicar tal conflito à Alta Administração da Puma e observar, de forma integral, a Política de Sigilo de Informações.

A Área de Compliance será responsável por determinar medidas mitigatórias ao caso específico, incluindo desde a restrição de acesso dos envolvidos aos documentos e às Informações Confidenciais da oferta em questão até a substituição provisória de profissionais.

2.4. Uso e Tratamento de Informações Confidenciais

Em observância às normas de autorregulação da Anbima, toda e qualquer Informação Confidencial (dado, documento ou informação) acessada por colaboradores em decorrência da coordenação de ofertas públicas deverá:

- (i) Ser utilizado única e exclusivamente para o estrito desenvolvimento do mandato e das atividades para as quais a Puma foi formalmente contratada, sendo terminantemente proibida a sua utilização para fins diversos, em benefício próprio ou de terceiros; e
- (ii) Ter sua confidencialidade integralmente mantida e resguardada até a regular e oficial divulgação dos documentos da respectiva oferta pública ao mercado, permanecendo vedada qualquer forma de exfiltração, compartilhamento ou uso fora dos termos autorizados da Operação.

Conforme tratado na Política de Investimentos Pessoais e em linha com os princípios do Código de Ética e Conduta, em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem:

- (i) **“Insider Trading”**, ou seja, a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores);
- (ii) **“Dica”**, ou seja, a transmissão, a qualquer terceiro, estranho às atividades da Coordenadora, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários; e/ou
- (iii) Front-running, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas aqui descritas 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 no Código de Ética e Conduta, nesta Política de Sigilo de Informações, na Política de Compliance e Controles Internos e na legislação aplicável, incluindo eventual demissão por justa causa.

3. MECANISMOS DE PROTEÇÃO E PREVENÇÃO

3.1. Regra Geral de Conduta e Vedações

A Puma realiza rigoroso controle de acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos em operações que exijam o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis no diretório de arquivos da

Puma, bem como que circulem em ambientes externos aos sistemas de informação homologados pela Coordenadora com estes arquivos, exceto quando não contiverem Informações Confidenciais, nos termos desta Política de Sigilo de Informações.

Nesse sentido, a título de exemplo, é vedado que quaisquer Colaboradores da Puma enviem arquivos com Informações Confidenciais por sistema de correio eletrônico diverso daquele utilizado pela Coordenadora, em conta de usuário não institucional, que criem cópias (digitais ou físicas) e façam *upload* a *drive* pessoal, enviem documentos para análise, resumo, revisão ou geração de conteúdo de inteligência artificial não contratada pela Puma, entre outras condutas aqui não especificadas que estejam em desacordo com os mecanismos, princípios e premissas desta Política de Sigilo de Informações.

A troca de informações entre os Colaboradores da Puma deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades, em benefício do princípio da Confidencialidade, e que não está sujeito a nenhuma barreira que impeça o seu recebimento.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Puma qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Coordenadora.

Sem prejuízo da Puma manter arquivo físico centralizado, também compete a cada Colaborador a responsabilidade pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

Somente é autorizada a destruição de documentos relacionados à atividade de coordenação da Puma (documentação regulatória, comunicações, correspondências, pareceres, relatórios etc.) (a) após o prazo de guarda legal, qual seja, 5 (cinco) anos, conforme previsão regulatória expressa (art. 21, Resolução CVM 161) e (b) com autorização expressa da Diretora de Compliance, Risco e PLD/FT.

Complementarmente, é autorizado o descarte de documentos físicos originais antes do vencimento do prazo supramencionado, desde que (a) tenha se procedido à correta digitalização, nos termos da lei e regulamentação vigente sobre o arquivamento e digitalização de documentos em meio eletrônico, e (b) não contenha nenhum erro

material de digitalização que prejudique a qualidade, integridade e legibilidade do documento em questão.

O descarte de Informações Confidenciais, quando permitido pela legislação e regulamentação aplicável e autorizado, em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar *pen drives*, HDs externos, fitas, discos pessoais ou quaisquer outros meios de reprodução particular e/ou armazenamento de informações que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Puma. A utilização desses equipamentos e outros análogos só é admitida quando (a) autorizada pela Área de Compliance, estritamente para os fins das atividades de coordenação da Puma, e (b) quando fornecido equipamento institucional próprio para esse fim, sendo vedado o uso de equipamentos pessoais. Caso não estejam satisfeitas ambas as condições, é proibida a conexão de equipamentos na rede da Puma.

A fim de se mitigar Riscos Cibernéticos, também é vedado que os Colaboradores da Coordenadora utilizem o equipamento de trabalho (computador institucional) para a visualização de sites, blogs, fotologs, webmails e redes sociais, entre outros, de cunho pessoal, bem como façam o download de arquivos particulares nos computadores de trabalho.

É de responsabilidade de cada Colaborador da Puma a integridade física (*hardware* e *software* inclusos) dos equipamentos fornecidos pela Coordenadora para o exercício da atividade profissional, estando sujeitos às sanções previstas nesta Política de Sigilo de Informações os casos em que ficarem constatados a culpa, culpa grave ou dolo do Colaborador em questão.

3.2. Acesso aos Sistemas e Instalações da Coordenadora

Para garantir a segurança e integridade das Informações Confidenciais, a Puma adota mecanismos robustos para acesso aos sistemas, incluindo autenticação de dois fatores, alteração periódica de senhas com critérios mínimos de complexidade, bem como monitoramento contínuo de acessos e tentativas de autenticação.

Para todo Colaborador da Coordenadora, será providenciado uma estação de trabalho móvel própria (*notebook*) e um login com usuário e senha institucional, exclusivamente para uso no exercício das atividades próprias da Coordenadora.

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, não devem ser compartilhadas e devem ser conhecidas somente pelo respectivo Colaborador usuário do computador, sendo pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros, mesmo que dentro da Coordenadora. Dessa forma, o Colaborador poderá ser responsabilizado, inclusive, caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Recomenda-se que, assim que recebidas, as senhas de acesso ao *notebook* e de usuário sejam trocadas por cada Colaborador. Adicionalmente, todas as senhas institucionais deverão ser trocadas, no mínimo, semestralmente, ou em prazo inferior determinado pela Diretora de Compliance, Risco e PLD/FT. A fim de se mitigar Riscos Cibernéticos, recomenda-se que sempre que trocadas, as senhas institucionais escolhidas não coincidam, aproximem-se, assemelhem-se ou compartilhem qualquer elemento em comum com as senhas pessoais do respectivo Colaborador.

Além disso, as instalações da Puma são protegidas por controles de acesso apropriados para garantir a segurança dos Colaboradores e proteger a confidencialidade, a integridade, rastreabilidade e a disponibilidade das Informações Confidenciais.

Cabe a cada Colaborador se certificar de que as sessões abertas e o acesso ao conteúdo armazenado no computador institucional de sua responsabilidade sejam devidamente bloqueados sempre que deixados sem supervisão.

A Puma permite o acesso remoto pelos Colaboradores ao e-mail, rede e diretório de arquivos corporativos, conforme requisição e autorização expressa da Área de Compliance. Os Colaboradores autorizados deverão (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso; (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos; (iii) relatar à Diretora de Compliance qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Coordenadora, seus clientes, prestadores de serviços e demais contrapartes e que ocorram durante o trabalho remoto; e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

A Puma mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Puma necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Coordenadora em caso de violação (“**Acesso Escalonado**”).

O acesso como “administrador” de área de desktop é limitado aos usuários aprovados pela Diretora de Compliance e PLD/FTP. Com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

Ademais, a concessão ou revogação de acesso aos diretórios de arquivos da Coordenadora deve seguir os seguintes critérios lógicos:

- (i) Os processos de gestão dos acessos devem ser conduzidos por um time responsável e especializado em tecnologia da informação, que tratará de qualquer sistema, independentemente de ser servidor interno ou externo (*drive*/nuvem);
- (ii) O acesso a qualquer sistema tecnológico deve ser protegido por credenciais de acesso, certificados, tokens, ou qualquer outro método seguro de identificação e dupla autenticação, sempre que possível, sendo esta obrigatória em acessos remotos;
- (iii) O acesso às informações e sistemas no âmbito das atividades desempenhadas pela Puma devem ser permitidos somente após um processo formal de autorização composto por, no mínimo, um registro feito pelo gestor do Colaborador solicitante à Área de Compliance;
- (iv) As credenciais de acesso a sistemas e informações, compostas por usuário e senha, devem ser concedidas pela Puma a Colaboradores e prestadores de serviço somente para o uso em atividades estritamente relacionadas ao exercício da atividade, pelo tempo em que perdurar seu vínculo com a empresa;
- (v) Os acessos dos Colaboradores e prestadores de serviços devem ser desativados quando eles forem desligados ou tiverem seus contratos de prestação de serviços encerrados;
- (vi) Todos os perfis de usuários para acesso às informações ou sistemas que contenham concentração de Informações Confidenciais devem ser revisados periodicamente pela Área de Compliance, observando o princípio de acesso mínimo e necessidade de conhecimento;
- (vii) O acesso lógico aos ativos de tecnologia da informação, tecnologia da automação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio da Puma deve ser sempre identificado, controlado e protegido, observando também o princípio da Rastreabilidade;

(viii) Em benefício do princípio da Confidencialidade, todas as credenciais devem conceder o acesso mínimo necessário para que o Colaborador exerça suas funções dentro da Puma;

(ix) Identidades de acesso genéricas ou de serviço nos ativos de tecnologia da informação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio da Puma são permitidas exclusivamente para integrações e/ou conexões; e

(x) Não é permitido que identidades genéricas e de serviços sejam utilizadas por Profissionais ou de fornecedores para fazer acesso a sistemas e/ou demais componentes de tecnologia ou automação. Qualquer exceção deve ser aprovada formalmente pela Diretoria de Controles Internos e Compliance.

3.3. Monitoramento

Independente de quaisquer comunicações ou constatações concretas de Riscos Cibernéticos, a Área de Compliance deverá adotar, em frequência trimestral, no mínimo, as seguintes medidas de monitoramento do uso de dados e sistemas da Coordenadora, como forma de prevenir e mitigar Riscos Cibernéticos ou outras violações potenciais:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a aplicativos de mensagens, bem como os e-mails enviados e recebidos;

(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Puma para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operações da Puma; e

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

A depender do contexto, a Área de Compliance está autorizada a aumentar a frequência ou a amostragem dos mecanismos de monitoramento ora previstos sem necessidade de edição desta Política de Sigilo de Informações.

3.4. Identificação e Reação à Riscos Cibernéticos

Em caso de quaisquer suspeitas de materialização de Risco Cibernético (infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Puma,

incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, a Diretora de Compliance, Risco e PLD/FT deverá ser cientificada por escrito prontamente.

Caberá à Diretora de Compliance, Risco e PLD/FT determinar quais membros da Alta Administração da Puma, estruturadores e investidores de ofertas públicas coordenadas pela Puma, prestadores de serviço, demais contrapartes e, conforme necessário em virtude do grau do Risco Cibernético, de agências reguladoras e de segurança pública, deverão ser notificados.

Qualquer Risco Cibernético apresentado ou identificado pela Área de Compliance deverá ser enfrentado na estrita observância dos seguintes critérios, respeitando a ordem:

- (i) Triagem e Diagnóstico. Avaliação imediata da natureza do incidente (ex.: infecção por malware, intrusão de rede, vazamento de credenciais), identificação das informações ou sistemas afetados e mensuração preliminar do impacto;
- (ii) Contenção e Isolamento. Identificação e desconexão imediata de sistemas, redes ou servidores comprometidos, visando estancar a propagação do ataque e proteger o perímetro tecnológico e informacional da Coordenadora;
- (iii) Mobilização. Acionamento imediato dos prestadores de serviços em tecnologia da informação;
- (iv) Erradicação e Restauração. Execução dos protocolos de recuperação, saneamento de vulnerabilidades e restauração dos sistemas e serviços prejudicados, prioritariamente aqueles que afetem as ofertas públicas coordenadas em andamento;
- (v) Notificação Regulatória e Comunicação: Avaliação e cumprimento das obrigações legais de notificação a terceiros, incluindo reguladores, autoridade de proteção de dados, clientes afetados e mercado, observando-se os prazos peremptórios da legislação vigente; e
- (vi) Investigação e Apuração de Responsabilidades. Condução de investigação interna liderada pela Área de Compliance para apurar as causas raiz do incidente. O relatório final será encaminhado à Alta Administração para a determinação de penalidades, acionamento de seguros e definição sobre a responsabilização pelas perdas financeiras decorrentes do evento, necessariamente instruído de provas materiais da conclusão.

3.5. Treinamento

É de responsabilidade da Área de Compliance oferecer treinamento de todo novo Colaborador da Puma acerca da proteção de dados pessoais, Informações Confidenciais e quaisquer outros dados sigilosos, nos termos desta Política de Sigilo de Informações

Periodicamente, com frequência mínima anual, o treinamento deverá ser reofertado a todos o Colaboradores da Coordenadora, podendo ser reavaliada a frequência mediante a necessidade de adequação as regras desta Política.

O treinamento referido neste item pode ser oferecido pela própria Diretora de Compliance e PLD/FTP, por outro membro da Área de Compliance por ela indicado ou por empresa terceirizada, em formato presencial, digital, síncrono ou assíncrono.

4. PROTEÇÃO E TRATAMENTO DE DADOS PESSOAIS

A Coordenadora reconhece a importância da privacidade e da proteção dos dados pessoais tratados no âmbito de suas atividades, observando integralmente o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - “**LGPD**”) e nas demais normas aplicáveis.

No exercício de suas funções, todos os Colaboradores devem garantir que a coleta, o uso, o armazenamento, o compartilhamento e a eliminação de “**Dados Pessoais**” e “**Dados Sensíveis**”, conforme definidos na LGPD, ocorram de forma segura, legítima e transparente, conforme as finalidades específicas da atividade desempenhada e os princípios previstos na LGPD.

A Coordenadora atua na qualidade de “**Controladora**” de Dados Pessoais, sendo responsável pelas decisões referentes ao tratamento de dados, e designa como Encarregada pelo Tratamento de Dados Pessoais (“Encarregada” ou “DPO”), nos termos do artigo 41 da LGPD, a Diretora de Compliance e PLD/FTP, que atua como canal de comunicação entre os titulares, a Coordenadora e a Autoridade Nacional de Proteção de Dados (“ANPD”).

Compete à Encarregada, nos termos do artigo 41, §2º, da LGPD: (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (ii) receber comunicações da ANPD e adotar providências; e (iii) orientar os Colaboradores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. A identidade e as informações de contato da Encarregada são divulgadas de forma clara e objetiva na página da Coordenadora na rede mundial de computadores, sendo o canal de contato o endereço de correio eletrônico compliance@pumacoordenadora.com.br.

Caso a reclamação, o incidente ou a suspeita de violação recaia sobre a própria Encarregada, o titular ou o Colaborador deverá reportar diretamente à Alta Administração, na forma prevista na Política de Compliance e Controles Internos.

Os Colaboradores comprometem-se a observar as orientações e instruções fornecidas pela Coordenadora quanto ao tratamento adequado de dados pessoais, bem como a notificar imediatamente a Área de Compliance e o Encarregado sobre qualquer incidente, suspeita de violação ou acesso indevido a informações pessoais.

A violação das regras de proteção de dados sujeitará o infrator às sanções disciplinares internas previstas na Política de Compliance e Controles Internos, sem prejuízo das responsabilidades civis, administrativas e criminais cabíveis.

5. DISPOSIÇÕES GERAIS

Esta Política de Sigilo de Informações, aprovada pela Alta Administração da Coordenadora, encontra-se disponível para consulta (i) mediante solicitação direta à Área de Compliance da Coordenadora; ou (ii) por intermédio da rede mundial de computadores, via website: <https://www.pumacoordenadora.com.br/documentos>.

Quaisquer dúvidas decorrentes desta Política de Sigilo de Informações poderão ser dirimidas pela Área de Compliance da Coordenadora, na Cidade de Ribeirão Preto, Estado de São Paulo, na Av. Braz Olaia Acosta, 727, sala 207, Jardim Califórnia, Ribeirão Preto, São Paulo, CEP 14026-040, por meio do endereço de correio eletrônico: compliance@pumacoordenadora.com.br.

6. HISTÓRICO DAS ATUALIZAÇÕES DA POLÍTICA DE SIGILO DE INFORMAÇÕES

Histórico das atualizações				
Data de Aprovação	Versão	Aprovação	Responsável	Periodicidade de Revisão
30 de setembro de 2026	1ª e atual	Alta Administração	Diretora de Compliance e PLD/FTP	Anual

ANEXO I

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, [--], inscrito no CPF/MF sob o nº [--] ("Colaborador"), da PUMA COORDENADORA DE OFERTAS PÚBLICAS LTDA., inscrita no CNPJ sob o nº 67.219.697/0001-67. ("Puma" ou "Coordenadora"), DECLARO para os devidos fins, estar ciente que:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("**Informações Confidenciais**"), quaisquer informações reservadas ou privilegiadas sobre a Puma, sua a atividade de coordenação, seus Colaboradores, clientes, prestadores de serviços e demais contrapartes (a) que não seriam normalmente obtidas por meio do acesso regular à rede mundial de computadores ou à diretórios de dados públicos, independentemente de estarem contidas em meios físicos ou digitais, e (b) que foram obtidas em razão de uma relação especial de confiança e prestação de serviço pela Puma, individual ou coletiva, direta ou indiretamente, incluindo, exemplificadamente:

- a) Informações pessoais de Colaboradores da Puma, de clientes, prestadores de serviços e demais contrapartes, tais como endereços, nomes, números cadastrais, informações financeiras e mais;
- b) Quaisquer informações envolvendo decisões de acionista controlador, deliberações de assembleia geral ou de órgãos de administração, bem como atos ou fatos de caráter político-administrativo, técnico, comercial ou econômico-financeiro relativos aos negócios da Puma ou de clientes, que possam ou não influir na cotação de valores mobiliários, na decisão de investidores de negociar tais ativos ou de exercer direitos a eles inerentes;
- c) Informações sobre resultados financeiros, balanços, balancetes e demonstrações financeiras da Coordenadora ou de clientes, antes de sua efetiva publicação e divulgação oficial ao mercado;
- d) Operações, negócios, parcerias ou transações financeiras e societárias realizadas ou em fase de negociação que ainda não tenham sido divulgadas publicamente;
- e) Estruturas organizacionais, planos de ação, metas de negócios, relações e listagens de clientes, contrapartes comerciais, investidores prospectados, fornecedores e prestadores de serviços;

- f) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e comerciais, incluindo saldos, extratos, movimentações, carteiras e posições de investimento de clientes;
- g) *Know-how*, metodologias de análise, técnicas de estruturação, cópias, diagramas, modelos de precificação, amostras, códigos-fonte e programas de computador proprietários ou customizados;
- h) Quaisquer dados, comunicações ou informações obtidas junto a sócios, diretores, colaboradores, estagiários e jovens aprendizes ou junto a seus assessores e consultores da Puma, que não tenham sido expressamente autorizadas para divulgação pública;
- i) Informações sobre o processo de sondagem de mercado (*market sounding*), *pilot fishing*, ordens de reserva, demandas, volumes, taxas de corte e intenções de investimento coletadas junto a investidores institucionais ou qualificados antes da precificação oficial da oferta;
- j) Quaisquer relatórios, questionários, auditorias jurídicas, financeiras ou socioambientais (ESG) e minutas de documentos da oferta (*prospectos*, lâminas, contratos de coordenação) gerados durante a fase de auditoria e estruturação de emissão e oferta; e
- k) Ofícios, cartas, exigências, consultas formais ou informais e respostas trocadas com a CVM, Anbima, B3 ou outras entidades administradoras de mercado organizado, cujo teor ou existência ainda não sejam públicos.

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

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

4. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.
5. A revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Coordenadora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.
6. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.
7. 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 e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Coordenadora são e permanecerão sendo propriedade exclusiva da Coordenadora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Coordenadora, devendo todos os documentos permanecer em poder e sob a custódia da Coordenadora, salvo se em virtude de interesses da Coordenadora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Coordenadora;
8. Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Coordenadora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e
9. 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 Coordenadora, 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.

10. 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 Coordenadora, permitindo que a Coordenadora procure a medida judicial cabível para atender ou evitar a revelação.

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

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

13. O Colaborador tem ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - “**LGPD**”) e se compromete a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas em conformidade com o estabelecido pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Coordenadora.

Ribeirão Preto-SP, [--] de [--] de [--].

[-Colaborador-]