



CÓDIGO DE ÉTICA E CONDUTA

DA

VLS LEGAL CAPITAL GESTÃO DE RECURSOS E INVESTIMENTOS LTDA.
CNPJ 56.604.951/0001-24

São Paulo
SETEMBRO DE 2026

O presente Código e todos os seus anexos foram elaborados pela VLS Legal Capital Gestão de Recursos e Investimentos Ltda. (“Gestora”) e não podem ser copiados, reproduzidos ou distribuídos sem prévia e expressa autorização desta.

CÓDIGO DE ÉTICA E CONDUTA

Código de Ética e Conduta (“Código”) da **VLS Legal Capital Gestão de Recursos e Investimentos Ltda.**, sociedade empresária limitada, inscrita no CNPJ sob o nº 56.604.951/0001-24, com sede na cidade e Estado de São Paulo, à Av. Presidente Juscelino Kubitschek, nº 360, sala 02, andar 09, conj. 91, Vila Nova Conceição, CEP 04.543-000 (“Gestora”).

I. INTRODUÇÃO

O presente Código estabelece as diretrizes e regras que devem ser observadas por todos os “Colaboradores” da Gestora, assim denominados os sócios e diretores, funcionários e quaisquer pessoas que possuam cargos, funções ou posições na Gestora, e tem por objetivo estabelecer os procedimentos, regras de Ética e Conduta e controles internos da Gestora, atendendo aos requisitos estipulados pela Comissão de Valores Mobiliários (“CVM”), bem como pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“ANBIMA”).

Tais diretrizes deverão ser compulsoriamente observadas pelos Colaboradores da Gestora, declarando estarem cientes de todas as regras e políticas aqui expostas, que lhes foram previamente apresentadas e em relação às quais não existe qualquer dúvida, comprometendo-se a observá-las, a todo tempo, no desempenho de suas atividades.

Em caso de dúvidas a respeito das disposições aqui contidas, o Colaborador deve consultar seu superior ou a Diretoria da Gestora.

II. DIRETRIZES NORTEADORAS DAS CONDUTAS

As ações e omissões ora abordadas não pretendem contemplar todas as situações possíveis relativas à ética e à conduta dos Colaboradores, porém, estabelecem os principais padrões que devem nortear as atividades de todos na Gestora.

Todos os Colaboradores da Gestora deverão agir com probidade, pautando suas condutas em conformidade com os valores de boa-fé e ética profissional, de forma a empregar no exercício de suas atividades o cuidado e diligência esperados de um profissional em sua posição, em relação aos clientes, às instituições com as quais a Gestora possua vínculo, bem como órgãos reguladores e fiscalizadores. Todos os Colaboradores devem conduzir suas ações, condutas e negócios de forma honesta e observar e obedecer às normas em vigor que afetem seus deveres profissionais e obedecê-las.

A Gestora e seus Colaboradores devem observar o disposto nas normas que regulamentam a atividade de gestão de recursos de terceiros, o Código de Administração e Gestão de Recursos de Terceiros da ANBIMA, bem como as demais normas regulatórias e autorregulatórias aplicáveis à atividade da Gestora, os procedimentos e

controles estabelecidos internamente e as orientações emanadas pelos órgãos reguladores e fiscalizadores competentes.

Os Colaboradores devem estar conscientes de que a informação transparente, precisa e oportuna constitui principal instrumento à disposição do cliente para que lhes seja assegurado o indispensável tratamento equitativo. Nenhum cliente deve ter tratamento preferencial por algum interesse ou sentimento de ordem pessoal de qualquer colaborador.

É estritamente proibido o recebimento ou o oferecimento de entretenimento, presentes ou benefícios de qualquer valor a/de agentes públicos, pessoas, entidades ou organizações públicas, salvo brindes institucionais de valor simbólico definido.

Com relação a funcionários, pessoas ou organizações particulares, de relacionamento comercial privado, é permitido o recebimento ou o oferecimento que em valor de até R\$ 3.000,00 (três mil reais) por pessoa, por presente. Presentes em dinheiro, em qualquer valor, são estritamente vedados.

Os Colaboradores deverão informar à Diretoria da Gestora sempre que se verifique, no exercício de suas atribuições, a ocorrência de violação à legislação ou às normas internas de conduta. O recebimento de qualquer reclamação deve ser informado à Diretoria, para que sejam tomadas as providências cabíveis.

III. TRATAMENTO DAS INFORMAÇÕES

A confidencialidade das informações é um princípio fundamental da Gestora que deve ser seguido por todos os seus Colaboradores, notadamente em relação a todas e quaisquer informações que venham a ter acesso durante o exercício das suas atividades na Gestora, incluindo aquelas disponibilizadas pelos sistemas e arquivos, bem como a informações não publicadas da Gestora, informações de clientes ou potenciais clientes, e aquelas obtidas de contratos com parceiros em que a Gestora se comprometeu a manter a confidencialidade. Este princípio se aplica às comunicações orais, escritas e impressas.

A armazenagem e a transmissão das informações, inclusive no que tange aos documentos e informações coletados de clientes, devem ser realizados de forma segura e controlada. A informação somente poderá ser acessada em ambiente seguro e por pessoas autorizadas com base no conceito *need-to-know*. Tal diligência se aplica também ao procedimento de descarte/destruição de informações, uma vez que o acesso e transmissão de informações pelos Colaboradores deverá ocorrer somente pelo período necessário para o desempenho das atividades, mantendo-as armazenada pelo prazo legal, bem como assegurando sua confidencialidade com base na classificação acima.

O descarte de informações sensíveis ou de documentos de guarda regulatória deve ser aprovado pela Diretoria; o descarte de informações de rotina segue procedimento interno,

sem aprovação individual. Arquivos digitais devem ser eliminados de forma irrecuperável, por meio de métodos adequados à mídia e ao ambiente de armazenamento. Os Colaboradores da Gestora deverão guardar absoluto sigilo sobre toda e qualquer informação, de natureza confidencial, a que tenham acesso ou conhecimento no desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados pela Gestora. Tal determinação se aplica igualmente às informações obtidas/repassadas verbal ou informalmente, assim como as escritas ou impressas.

Os Colaboradores da Gestora deverão:

- (i) advertir, de forma clara, àqueles em relação a quem se verificar a necessidade de revelar informação não pública, sobre a responsabilidade pelo cumprimento do dever de sigilo e pela proibição legal de que se utilizem de tal informação para obter, em benefício próprio ou alheio, vantagem indevida;
- (ii) guardar sigilo sobre qualquer informação a que tenham acesso e que ainda não tenha sido divulgada ao público em geral, ressalvada a revelação da informação quando necessária para a Gestora conduzir seus negócios de maneira eficaz e, ainda, somente se não houver motivos ou indícios para presumir que o receptor da informação a utilizará erroneamente; e
- (iii) se abster de emitir opiniões que possam ser consideradas discriminatórias, racistas, sexistas, homofóbicas, xenofóbicas, extremistas, violentas ou que possam prejudicar a imagem da Gestora violar os direitos de terceiros. Além disso, os Colaboradores devem evitar emitir opiniões políticas ou religiosas que possam causar desconforto ou divisão entre os Colaboradores, clientes e parceiros da Gestora, a menos que sejam previamente aprovadas pela Diretoria da Gestora.

O fornecimento de informações não públicas a não colaboradoras da Gestora será realizado somente nos casos estritamente necessários a fim de cumprir as normas atinentes à atividade desenvolvida pela Gestora, para a proteção contra fraudes ou qualquer outra atividade ilegal suspeita, mediante contratos de confidencialidade, quando for o caso.

Em nenhuma circunstância, os Colaboradores da Gestora poderão utilizar informações confidenciais para ganho pessoal, nem as fornecer a terceiros, inclusive familiares, parentes e amigos, ou a outros Colaboradores da Gestora que não necessitem delas para suas atividades.

Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, procurar a Diretoria da Gestora para obter orientação adequada, devendo ser atribuída interpretação extensiva ao conceito de informação confidencial definido acima.

A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada à Diretoria da Gestora para que seja decidida a forma mais adequada para tal revelação.

A manutenção da confidencialidade das informações às quais os Colaboradores tiverem acesso deve perdurar durante toda a existência da Gestora, bem como após o desligamento dos Colaboradores. Este compromisso abrange a obrigação de confidencialidade pactuada com as instituições contratantes, observados os prazos definidos nos respectivos contratos firmados entre as partes.

Os Colaboradores reconhecem que os negócios da Gestora são altamente competitivos e por isso declaram e reconhecem que estão impedidos de abordar, direta ou indiretamente, os clientes da Gestora. Após o desligamento da Gestora, o Colaborador mantém o compromisso de não abordar os clientes da Gestora inclusive por interposta pessoa, assim como não prosseguir com qualquer abordagem caso identifique essa restrição quando de eventual contato, pelo prazo de 24 (vinte e quatro) meses contados da data em que deixou de ser Colaborador da Gestora.

É vedado o aliciamento de qualquer colaborador, prestador de serviço ou sócio da Gestora enquanto for colaborador da Gestora, bem como pelo prazo de 24 (vinte e quatro) meses do seu desligamento, assim como a constituição de novo negócio potencialmente concorrente com qualquer integrante do quadro de sócios da Gestora observado o mesmo prazo.

IV. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Funções e Responsabilidades

Os Colaboradores da Gestora que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado, devendo salvaguardar as senhas e outros meios de acesso aos mesmos. Considerando que os Colaboradores terão acesso à informação de acordo com o conceito “*need-to-know*”, adiante definido, a função exercida pelo Colaborador dentro da Gestora estará estreitamente relacionada ao volume e sensibilidade das informações as quais lhe será dado acesso e, conseqüentemente, relacionada à responsabilidade do Colaborador perante a informação. Desta forma, os Colaboradores que tenham acesso aos ativos de informação da Gestora serão imediatamente responsáveis pela salvaguarda de todo o sistema informacional.

A base de dados eletrônicos utilizada pela Gestora é segregada de modo que informações confidenciais sejam arquivadas em pastas de acesso restrito, acessada pelos usuários previamente autorizados.

O compartilhamento de dados pessoais e informações classificadas como Confidenciais entre os Colaboradores da Gestora deve sempre observar o princípio de que o destinatário

necessita daquelas informações para o desempenho de suas atividades (“*need-to-know*”) e que não estará sujeito a nenhuma restrição que impeça o recebimento daquelas informações.

A Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018 – e legislação correlata foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo e versa sobre a coleta, tratamento, tratamento e compartilhamento de dados das pessoas naturais ou jurídicas, de direito público ou privado, e sobre o sigilo de informações por meios manuais ou digitais (“Dados”).

A Gestora e seus Colaboradores comprometem-se a observar os mais elevados critérios e padrões de conduta profissional, em plena conformidade com a Legislação Aplicável. A Gestora e seus Colaboradores também têm a obrigação de garantir que os Dados sejam utilizados exclusivamente para as finalidades que motivaram sua obtenção, de forma limitada e compatível com os objetivos definidos em observância à legislação vigente.

O compartilhamento de Dados somente será permitido: (i) entre Colaboradores da Gestora, quando necessário à condução de seus negócios; ou (ii) com reguladores, ou quando exigido por lei, norma, regulamento ou ordem judicial emanada de tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo, desde que a Diretoria da Gestora seja previamente consultada.

Gerenciamento de Identidade e Acesso

Todos os computadores da Gestora possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores utilizados pela Gestora permitem a identificação do seu remetente/receptor.

No caso de admissão de novo Colaborador será criado perfil de acesso e senha pessoais e intransferíveis para o novo Colaborador. Este perfil somente dará acesso às informações apropriadas para ciência do novo Colaborador, e a modificação e/ou revogação de suas permissões só poderá ser feita mediante autorização formal de qualquer membro da Diretoria da Gestora. O login e a senha (respeitada as regras de alteração e sua periodicidade) acompanham o Colaborador até sua saída da Gestora, momento em que serão imediatamente bloqueados.

O acesso aos sistemas e arquivos é restrito por usuário e perfil, conforme o padrão de segurança definido pela área de TI. A construção das senhas de acesso será feita através de lógica confidencial estabelecida pela Diretoria, e conterà, necessariamente, no mínimo 8 (oito) caracteres, sendo no mínimo 1 (uma) letra, 1 (um) número e 1 (um) caractere especial. Os sistemas devem adotar mecanismos de proteção contra tentativas de acesso não autorizado, tais como autenticação multifator e bloqueio ou limitação de tentativas

sucessivas de autenticação, cabendo à área de TI definir os parâmetros e o procedimento de desbloqueio. Anualmente serão revistos os perfis existentes, inclusive os bloqueados, a fim de checar eventual irregularidade de acessos.

Gestão de Comunicações Eletrônicas

O sistema eletrônico utilizado pela Gestora está sujeito à revisão, monitoramento e gravação a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

A Gestora se reserva ao direito de monitorar os recursos de infraestrutura de informação, como softwares ou equipamentos, incluindo os computadores, internet, chat e linhas telefônicas, ficando, a seu exclusivo critério e sem a necessidade de aviso prévio, gravar qualquer ligação telefônica dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela Gestora.

Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores. Da mesma forma, toda e qualquer comunicação trocadas por qualquer sistema de mensagem instantânea com clientes poderá ser monitorada ou solicitada para os Colaboradores.

Os Colaboradores deverão informar imediatamente à Diretoria caso, no exercício de suas atribuições, suspeitem ou encontrarem indícios da violação desta Política ou da ocorrência de incidentes de segurança, tais como vazamento de senhas, perda ou extravio de informações e documentos, inclusive nos casos em que outro colaborador, ou ele mesmo, possa ter dado causa à ocorrência de incidentes. O recebimento de qualquer reclamação deve ser informado à Diretoria, para que sejam tomadas as providências cabíveis no prazo máximo de 5 (cinco) dias.

Proteção de Computadores e Redes

Todos os programas de computador utilizados pelos Colaboradores devem ser licenciados e ter sido previamente autorizados. Downloads de qualquer natureza, excetuados os de programas de computador, podem ser realizados, desde que de forma justificada. Poderão ser realizadas inspeções nos equipamentos, mediante necessidade, para averiguação de uso indevido.

A cópia de arquivos e instalação de programas em computadores da Gestora deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

Os computadores devem contar com firewall e proteção contra código malicioso, configurados e gerenciados pelos prestadores de serviço de TI.

É estritamente vedado aos Colaboradores, acessar, através dos computadores, perfis e/ou usuários da Gestora, sites que contenham conteúdos inapropriados para o ambiente de trabalho.

Os Colaboradores não poderão acessar os sistemas da Gestora de local diverso da estação de trabalho, inclusive por dispositivos móveis, salvo se autorizado pela Diretoria, de forma prévia e expressa, por qualquer meio de comunicação que se comprove sua entrega.

Os Colaboradores que tiverem acesso aos sistemas de informação e plataformas de negociação serão responsáveis por:

- (i) manusear a informação protegida de forma apropriada, sendo vedado o acesso a informações protegidas por meio de rede não protegida;
- (ii) suas ações associadas ao uso que fazem da informação protegida;
- (iii) reportar à Diretoria e ao Agente de Segurança/TI designado pela Gestora qualquer suspeita ou conhecimento de violação desta política ou incidente de segurança da informação. Qualquer vazamento de informações de clientes ou de Colaboradores deve ser relatado;
- (iv) assegurar que conhecem e cumprem as políticas, as normas e as diretrizes aplicáveis às suas responsabilidades; e
- (v) não utilizar informações a que tiveram acesso em função das suas atividades ou cargo na Gestora para seu ganho pessoal, familiar ou de terceiros; e divulgar informações sobre a Gestora, seus clientes e negócios a partes não autorizadas, inclusive por meio de mídias sociais externas.

Os colaboradores devem manter os documentos de trabalho armazenados no Sharepoint/OneDrive corporativo. Os documentos de trabalho armazenados nas pastas indicadas, são objeto de *back-up* diário em ambiente protegido e criptografado no Brasil com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização, sendo o teste de recuperação de back-up realizado anualmente, de forma integrada ao teste de ativação do Plano de Contingência.

O *back-up* em ambiente de nuvem implica na necessidade de acesso à informação protegida armazenada no datacenter do prestador de serviço fornecido por meio de funcionalidade de autenticação de duplo-fator, sendo a informação protegida criptografada quando em repouso ou transmitida por meio da internet.

O acesso de informações protegidas via nuvem deve estar restrito aos Colaboradores autorizados pela Gestora.

É vedada a contratação de serviço de e-mail externo gratuito. Para a contratação deste serviço, a Gestora deverá obter seu domínio próprio, ficando disponível a funcionalidade de criptografia ou forma alternativa de proteção da informação.

O descarte de informações não públicas deve observar as seguintes diretrizes:

- (i) ao expirar o prazo aplicável de retenção da informação protegida, esta deverá ser apagada e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
- (ii) os documentos físicos que contenham informação protegida devem ser triturados por fragmentadora imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
- (iii) a eliminação ou a destruição final das mídias ou dos documentos, realizada por terceiros, que contenham informação protegida deve ser documentada. A contratação de terceiros para tanto implica na necessidade de observância da Política de Segurança de Informação;
- (iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Gestora devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

V. UTILIZAÇÃO DE BENS E EQUIPAMENTOS

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina a fins profissionais. Redes sociais e sites de relacionamento deverão ser acessados apenas caso haja necessidade para execução das atividades profissionais. O uso indiscriminado pelos Colaboradores para fins pessoais deve ser evitado, e nunca deve ser prioridade em relação a qualquer utilização profissional.

E-mails ou quaisquer outras modalidades de sistemas de comunicação devem ser utilizadas somente para os negócios da Gestora. Neste sentido, é proibido:

- (i) enviar mensagens eletrônicas com informações confidenciais para endereços externos à Gestora;
- (ii) enviar mensagens eletrônicas com anúncios de eventos particulares, propagandas, opiniões pessoais, vídeos, músicas, campanhas ou promoções;

- (iii) utilizar o e-mail corporativo para participação em fóruns e listas de discussão não relacionados às atividades do colaborador, ou mesmo, utilizar para cadastro em sites de redes sociais, e-commerce, entre outros;
- (iv) transmitir material que seja considerado ofensivo, discriminatório, calunioso, fraudatório, danoso, ilegal ou que possa violar os padrões de ética e cortesia profissional.

A consulta, envio ou repasse de conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails ou mensagens com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Gestora.

VI. PROTEÇÃO DE DADOS PESSOAIS

O presente Capítulo visa regular o tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Gestora, assim considerada toda operação realizada com tais dados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Além do presente Código, todos os Colaboradores devem observar as políticas internas adotadas pela Gestora e empresas ligadas, às quais foram apresentados quando de suas entradas na Gestora. As versões atualizadas das políticas e manuais encontram-se disponíveis no repositório oficial de normas internas, bem como foram devidamente enviadas a cada um dos Colaboradores.

Consideram-se “Dados Pessoais” qualquer informação relacionada a pessoa natural identificada ou identificável. Deste modo, sujeitam-se à tutela desta Política todos os Dados Pessoais de Colaboradores, investidores, parceiros, prestadores de serviço ou quaisquer terceiros com os quais a Gestora mantenha relacionamento de qualquer natureza. São considerados, ainda, Dados Pessoais aqueles utilizados para formação de perfil comportamental de determinada pessoa natural, se identificada.

Consideram-se “Dados Pessoais Sensíveis” os Dados Pessoais que versem sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

Todos os Dados Pessoais ou Dados Pessoais Sensíveis são informações confidenciais e devem ser tratados como tal para os fins deste Código.

Deste modo, as seguintes condutas são vedadas aos Colaboradores:

- (i) envio de informações para e-mail pessoal;

- (ii) armazenamento de informações em mídias removíveis;
- (iii) processamento e armazenamento de informações em repositórios em nuvem ou em infraestrutura de terceiros, exceto quando existir um contrato de prestação de serviço, bem como cláusulas de confidencialidade definidas; e
- (iv) compartilhamento com terceiros por quaisquer meios.

As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

- (i) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- (ii) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- (iii) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- (iv) Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;
- (v) Qualidade dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- (vi) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- (vii) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- (viii) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;
- (ix) Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

(x) Responsabilização e Prestação de Contas: demonstração, pela Gestora, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas. O tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Gestora só será realizado nas seguintes hipóteses:

- (i) para o cumprimento de obrigação legal ou regulatória;
- (ii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- (iii) quando necessário para atender aos interesses legítimos da Gestora ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais e Dados Pessoais Sensíveis;
- (iv) mediante o fornecimento de consentimento pelo titular por escrito ou outro meio que demonstre a manifestação de vontade do titular; ou
- (v) para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

O legítimo interesse da Gestora poderá ter fundamento, mas não se limita, às seguintes finalidades:

- (i) apoio e promoção de atividades da Gestora; e
- (ii) proteção, em relação ao titular, do exercício regular dos seus direitos ou prestação de serviços que o beneficie, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

No caso de interesse legítimo, somente os Dados Pessoais e Dados Pessoais Sensíveis estritamente necessários serão tratados, sendo outorgada ampla transparência ao titular sobre o tratamento implementado.

O consentimento deve observar as seguintes diretrizes:

- (i) se outorgado por escrito deverá constar de cláusula destacada das demais cláusulas contratuais;
- (ii) o Dado Pessoal obtido mediante consentimento do titular só poderá ser compartilhado com terceiros se houver expressa autorização do titular;
- (iii) o consentimento deve referir-se a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados. Caso alterada a finalidade,

deverá ser coletado novo consentimento do titular;

(iv) o consentimento poderá ser revogado a qualquer tempo por manifestação expressa do titular, por procedimento gratuito e facilitado, ratificado o tratamento realizado ao amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação dos dados.

A Gestora outorgará ao titular o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que serão disponibilizadas de forma clara, adequada e ostensiva, incluindo as seguintes informações:

(i) finalidade específica do tratamento, ratificando que o tratamento de Dados Pessoais é condição para o fornecimento do serviço de gestão profissional de recursos em virtude de obrigação regulatória;

(ii) forma e duração do tratamento, observados os segredos comercial e industrial;

(iii) identificação e informações de contato da Gestora que atuará como controladora da informação;

(iv) informações acerca do potencial compartilhamento de dados pela Gestora e a sua finalidade;

(v) responsabilidades dos Colaboradores que realizarão o tratamento; e

(vi) informações sobre os direitos do titular, na forma do art. 18 da Lei Geral de Proteção de Dados, e meios pelos quais tais direitos poderão ser exercidos.

O término do tratamento de Dados Pessoais e Dados Pessoais Sensíveis ocorrerá nas seguintes hipóteses:

(i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

(ii) fim do período de tratamento, ou seja, 05 (cinco) anos após a cessação da prestação de serviço ao titular;

(iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou

(iv) determinação da autoridade nacional, quando houver violação da Lei Geral de Proteção de Dados.

Os Dados Pessoais e Dados Pessoais Sensíveis serão eliminados após o término de seu

tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

- (i) cumprimento de obrigação legal ou regulatória
- (ii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos acima; ou
- (iii) uso exclusivo da Gestora, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A Gestora manterá registro das operações de tratamento de Dados Pessoais e Dados Pessoais Sensíveis que realizar, especialmente quando baseado no seu legítimo interesse.

A Autoridade Nacional de Proteção de Dados poderá determinar que a Gestora elabore um relatório de impacto à proteção de Dados Pessoais, inclusive Dados Pessoais Sensíveis, referente às operações de tratamento de dados. Este relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise da Gestora sobre estas medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O encarregado pelo tratamento de Dados Pessoais e Dados Pessoais Sensíveis será identificado no site da Gestora, assim como as suas informações para contato.

VII. PROCESSO DE CADASTRO E *KNOW YOUR CLIENT*

Os Colaboradores devem seguir, rigorosamente, os procedimentos de cadastro, “*Conheça seu Cliente*” e *Suitability*, conforme definido na Resolução CVM 30.

A Gestora deve valer-se dos documentos e formulários recebidos, incluindo ficha cadastral, termo de adesão, termo de ciência de risco, declaração da condição de investidor qualificado/profissional, formulário de *suitability*, bem como quaisquer outros documentos. Tais documentos deverão ser digitalizados e enviados por e-mail, previamente à aplicação pelo cliente, em conjunto com a documentação complementar eventualmente exigida para fins de comprovação das informações prestadas. Cabe aos Colaboradores a orientação dos clientes com relação à necessidade de preenchimento de forma completa, consistente, legível e sem rasuras.

Sem prejuízo do envio da documentação indicada no item acima, a Gestora manterá tais informações em seus arquivos, de forma organizada e atualizada, em meio digital ou físico, por quanto perdurar como cliente, e, posteriormente, armazenar as informações pelo prazo mínimo de 5 (cinco) anos após o encerramento da conta.

Com relação ao processo de “Conheça o seu Cliente”, os Colaboradores deverão valer-se de pesquisas na internet através do site de busca (www.google.com.br) a fim de identificar

eventuais informações desabonadoras relacionadas ao cliente e potenciais riscos à Gestora, bem como colaborar para a sua identificação. Caso identificado qualquer risco, ainda que em potencial, os Colaboradores avaliarão se a operação é passível de comunicação ao COAF.

Caso haja qualquer dúvida ou suspeita com relação à veracidade das informações prestadas ou idoneidade do cliente, não sanada após a solicitação de esclarecimentos adicionais, a Gestora deverá abster-se de seguir com a operação.

Para fins de Cadastro de Colaboradores (“*Know your Employee*”), a Gestora adotará uma postura rígida e transparente na vinculação de sócios e contratação de seus funcionários. Antes do ingresso na Gestora, todos os interessados deverão ser entrevistados. Requisitos ligados à reputação no mercado e perfil são avaliados, bem como antecedentes profissionais.

VIII. POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO

A prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (“PLD/FTP”) é objeto de extensas normas editadas por órgãos governamentais que impõem uma série de requerimentos e exigências a diversos participantes do mercado financeiro e de capitais, a fim de detectar e prevenir potenciais atividades de lavagem e ocultação de bens.

Com este objetivo, os Colaboradores da Gestora deverão observar e cumprir as regras e procedimentos melhor descritos e definidos na PLD/FTP, documento apartado e complementar ao presente Código, relacionados à prevenção à lavagem de dinheiro e financiamento do terrorismo, assim como aplicar esforços para determinar a verdadeira identidade de todos os seus clientes, incluindo informações e documentos que comprovem a sua situação financeira e patrimonial.

IX. ALTA ADMINISTRAÇÃO DA VLS LEGAL CAPITAL

A Alta Administração, conforme conceito dado pela Res. CVM 50, é o órgão decisório máximo da Gestora, responsável pelos assuntos estratégicos e pelo cumprimento de regras, políticas, procedimentos e controles da Gestora, comprometendo-se com a efetividade e adequação do presente Código e das demais políticas, manuais e controles internos da Gestora.

A Alta Administração da Gestora é composta por pessoas naturais que reúnem a expertise e a capacidade técnica para exercer suas respectivas funções.

A Alta Administração é formada pelos diretores: (i) Gilberto Martins Cordeiro, que atua como diretor da Gestora; (ii) Renata Pinheiro Ferreira Rodrigues, que ocupa o cargo de Diretora de Risco e Compliance da Gestora; e (iii) Henrique Belcastro de Almeida, que

ocupa o cargo de Diretor Administrador de Carteiras da Gestora, autorizado pela CVM por meio do Ato Declaratório nº 25.096, de 10 de abril de 2026 (“Diretores”).

Os Diretores da Gestora também conduzirão uma revisão anual do presente Código, assim como deliberar, sempre quando necessário, sobre qualquer ocorrência de atividade atípica, suspeita ou contrária ao presente Código.

Dentre as responsabilidades dos Diretores da Gestora, destacam-se as seguintes: (i) servir como pessoas de contato para todas as solicitações de informações, internas ou externas, relacionadas à PLD/FTP; (ii) supervisionar a estrutura para procedimentos e controles instituídos pela Gestora; e (iii) observar à política de PLD/FTP de todos aqueles a que a Gestora esteja vinculada, simultaneamente, devendo reportar as propostas ou ocorrências das operações ou situações atípicas, dentro do limite de suas atribuições.

X. POLÍTICA DE TREINAMENTO

A Gestora conta com um programa de treinamento dos Colaboradores dividido em 02 (duas) etapas distintas (“Programa de Treinamento”). A primeira etapa consiste na apresentação dos normativos internos ao colaborador no ato do seu ingresso na Gestora e, a segunda, mediante treinamento anual da equipe sobre os procedimentos e controles internos, incluindo o adequado tratamento às informações confidenciais e tratamento de dados pessoais, abordando aspectos como: (i) natureza; (ii) escopo; (iii) finalidade; (iv) probabilidade e a gravidade de riscos; (v) benefícios decorrentes do tratamento de dados.

Sem prejuízo dos treinamentos internos, os Colaboradores poderão ser submetidos a treinamentos, os quais deverão ser implementados nos prazos por esta definidos, sendo arquivadas as evidências da sua realização pelo prazo mínimo de 5 (cinco) anos.

XI. POLÍTICA ANTICORRUPÇÃO

É terminantemente proibido aos Colaboradores, atuando por si ou por meio de terceiros, praticar atos lesivos contra a administração pública, nacional ou estrangeira, que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil.

É terminantemente proibido ao Colaborador, agindo em seu nome ou em nome da Gestora, dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento de, direta ou indiretamente, qualquer dinheiro ou qualquer coisa de valor a qualquer servidor público, autoridade governamental, consultores, representantes, parceiros, ou quaisquer terceiros, com a finalidade de influenciar qualquer ato ou decisão do agente ou do governo, ou para assegurar qualquer vantagem indevida, ou direcionar negócios para, qualquer pessoa, e que violem as regras das normas anticorrupção.

A Gestora ou seus Colaboradores não deverão praticar atos que possam ser direta ou indiretamente entendidos como tentativa de suborno, aceitação de suborno ou envolvimento em atividades de corrupção, junto ao setor público e privado.

O Colaborador deverá atentar, ainda, que qualquer valor oferecido a agentes públicos, por menor que seja e independentemente da aceitação pela agente público, poderá ensejar a aplicação das penalidades previstas nas normas anticorrupção à Gestora, hipótese em que o colaborador estará sujeito a indenizar a Gestora, por meio das medidas legais cabíveis.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou agentes públicos que não encontram previsão legal ou regulamentar. Quaisquer pagamentos que não sejam anotados nos livro-caixa ou nos registros contábeis da Gestora são vedados.

Sem prejuízo das orientações acima, os Colaboradores deverão observar as seguintes diretrizes:

- (i) não defraudar, manipular ou impedir processos de ofertas públicas ou a execução de contratos administrativos;
- (ii) não criar dificuldades ou retardar procedimentos de investigação do governo.

Nenhum Colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

A Gestora e seus Colaboradores devem ainda verificar, na contratação e mediante consulta a fontes públicas, se terceiros prestadores de serviços e parceiros comerciais respondem a processos ou foram condenados por práticas corruptivas, com reverificação periódica dos prestadores e parceiros relevantes, conforme a sua classificação de risco, ou diante de alerta de risco, devendo abster-se de manter relacionamento ou contratar terceiros se houver sérios indícios ou condenação em casos de corrupção ativa ou passiva.

Qualquer suspeita ou indício de práticas corruptivas por parte de Colaboradores da Gestora deve ser comunicada imediatamente à Diretoria.

XII. PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade de Negócios tem como objetivo assegurar a continuidade das operações na eventualidade de uma indisponibilidade prolongada dos recursos essenciais (pessoas, dados, sistemas de informação, equipamentos e instalações), e é composto pelas seguintes fases:

Identificação das Atividades Essenciais: as atividades essenciais ao objeto social são todas aquelas que compõem o processo de (i) prospecção e captação de clientes; (ii)

recepção e registro de ordens e transmissão destas para os sistemas de negociação ou de registro cabíveis, na forma da regulamentação em vigor e instruções das instituições contratantes; e (iii) prestação de informações sobre os produtos oferecidos e sobre os serviços prestados pelas instituições contratantes.

A continuidade das atividades essenciais acima mencionadas é garantida mediante o arquivamento das informações e registros relacionados a estes processos em ambiente seguro, com acesso restrito aos integrantes da equipe, e objeto de backup, possibilitando o acesso através de outro por meio de dispositivo autorizado, mediante credencial de uso individual e autenticação multifator

Identificação da Interrupção do Funcionamento dos Recursos: no caso de (i) perda do espaço de trabalho; (ii) impossibilidade de acesso às dependências por motivos de força maior; (iii) indisponibilidade de pessoal; (iv) indisponibilidade de recursos de tecnologia; ou (v) ataques cibernéticos; a Diretoria orientará os Colaboradores sobre a postura e providências cabíveis, de acordo com a natureza e gravidade da contingência.

Ativação do Plano e Acesso às Informações para Continuidade das Operações Críticas: a ativação do Plano de Contingência consiste no acesso pelos Colaboradores aos dados e informações necessárias ao desempenho das respectivas atividades, através de local diverso da sede social.

Todos os sistemas da Gestora são passíveis de ser acessados de qualquer localidade, desde que efetuado acesso por meio de dispositivo autorizado, mediante credencial de uso individual e autenticação multifator.

Testes Periódicos: anualmente serão realizados testes de ativação do Plano de Contingência, que incluem a verificação do back-up e do tempo de *restore*.

Tal como configurados os recursos disponíveis atualmente, o tempo máximo previsto de absoluta falta de acesso aos recursos essenciais é de 1 (um) dia útil, sendo considerado, para tal cômputo, o tempo de deslocamento da sede da Gestora a outra estação que possua equipamento com segurança satisfatória.

Comunicação: em qualquer situação de indisponibilidade ou instabilidade dos recursos essenciais, inclusive de percepção de evidências de futura situação de indisponibilidade, os membros da Diretoria serão os primeiros a serem comunicados. A comunicação deve ser buscada pelos meios a seguir relacionados, em ordem de tentativas, prioritariamente por e-mail diferente do afetado e alternativamente através de aparelho móvel relacionado às atividades do trabalho, ou conforme definido pela Diretoria. Esses dados serão disponibilizados pelos membros da Diretoria diretamente aos Colaboradores depois dos treinamentos descritos neste Código.

XIII. MEDIDAS ADICIONAIS DE GOVERNANÇA E CONFORMIDADE

A Gestora, em linha com os princípios de ética, integridade e aderência regulatória, implementará um conjunto de medidas com o objetivo de reforçar seus controles internos e garantir a prevenção de inconsistências cadastrais e operacionais.

Dentre as medidas adotadas, destacam-se:

- (i) Implementação de revisão periódica conforme a classificação de risco de cada cliente, observado o intervalo máximo de 5 (cinco) anos previsto na Resolução CVM nº 50/2021, dos dados sensíveis dos clientes;
- (ii) Reforço do programa de compliance e LGPD, com atualização de políticas internas e treinamentos; e
- (iii) Nomeação formal de responsável por compliance regulatório, que pode ser a própria Diretora de Risco e Compliance.

Essas ações refletem o compromisso permanente da Gestora com a conformidade legal, regulatória e contratual, bem como com a transparência perante seus clientes e parceiros.

XIV. COMUNICAÇÃO COM A IMPRENSA E USO DE REDES SOCIAIS

Visando o resguardo dos interesses da Gestora em face ao volume de informações com as quais precisa lidar diariamente, somente a Diretoria, ou pessoa prévia e expressamente autorizada, pode manter qualquer tipo de comunicação, em nome da Gestora, com jornalistas, repórteres, entrevistadores ou agentes da imprensa falada ou escrita (“Imprensa”).

Os Colaboradores autorizados a participar de entrevistas e assemelhados deverão restringir-se a tecer comentários estritamente técnicos, evitando o uso de juízos de valor desnecessários, devendo pautar suas declarações na cautela. O Colaborador não deve se manifestar em meios de comunicação ou mídias sociais opiniões que possam ser interpretadas como posição oficial da Gestora.

Os Colaboradores não devem inserir imagens ou informações nas redes sociais, que possam identificar pessoas, instituições, clientes e não-clientes sem sua prévia e expressa autorização.

É vedado, sob qualquer circunstância, conceder declaração à Imprensa que possa aparentar ou ter conteúdo discriminatório em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei, assim como a utilização de expressões de baixo calão ou não condizentes com a melhor educação.

É vedado, sob qualquer circunstância, conceder declaração à Imprensa que possa aparentar ou possuir orientação político-partidária.

XV. DISPOSIÇÕES GERAIS E ENFORCEMENT

O presente Código prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os Colaboradores da Gestora aos seus termos e condições.

O presente Código será revisado sempre que a Diretoria julgar necessário, em razão, exemplificativamente: do início de relacionamento com novos clientes e instituições; da verificação de falhas ou brechas nas políticas; e de mudanças na legislação aplicável. Cada atualização do Código deverá ser representada no histórico de versões.

A título de *enforcement*, vale notar que a não observância dos dispositivos do presente Código resultará em advertência, suspensão ou demissão/exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.

* * * * *

ANEXO I

TERMO DE ADESÃO AO CÓDIGO DE ÉTICA E CONDUTA DA VLS LEGAL CAPITAL GESTÃO DE RECURSOS E INVESTIMENTOS LTDA.

(“VLS Legal Capital”)

Pelo presente, [qualificação completa], declara que:

1. recebeu cópia e treinamento a respeito do Código de Ética e Conduta, incluindo todas as Políticas neles contidas, tendo compreendido a integralidade dos seus termos e disposições, comprometendo-se a cumpri-lo e observá-lo no dia a dia das suas atividades, observadas as limitações das funções desempenhadas por cada colaborador na VLS Legal Capital;
2. está ciente que durante o exercício das atividades profissionais na VLS Legal Capital poderá ter acesso a informações confidenciais, conforme definição constante do Código de Ética e Conduta, devendo, portanto, mesmo após eventual desligamento da VLS Legal Capital, guardar o devido sigilo em relação às citadas informações, observando as regras de conduta atinentes ao correto tratamento de informações confidenciais descritas no Código;
3. está ciente e de acordo que todos os documentos relacionados direta ou indiretamente às atividades da VLS Legal Capital, sejam confidenciais ou não, inclusive, mas não limitando-se aos contratos, e-mails e demais correspondências, arquivos, sistemas, planilhas banco de dados, cadastro e informações de clientes, obtidos e/ou desenvolvidos em decorrência do desempenho das atividades profissionais são de exclusiva propriedade da VLS Legal Capital, razão pela qual compromete-se a não utilizar tais documentos para quaisquer fins que não o desempenho das suas atividades profissionais;
4. a VLS Legal Capital está autorizada ao tratamento dos seus dados pessoais, sensíveis ou não, para fins de cumprimento das leis e normas que regem as suas atividades, bem como quando necessário para atendimento dos seus interesses legítimos, proteção da sua reputação e imagem, ou de seus clientes. O consentimento ora outorgado poderá ser revogado pelo colaborador, não afetando, entretanto, a legalidade de nenhum tratamento realizado em momento anterior à revogação, bem como o tratamento lícito dispensado da necessidade de consentimento;
5. a VLS Legal Capital está autorizada a realizar verificações ou pesquisas independentes utilizando seu nome e documentos, com base em informações disponíveis publicamente;

6. está ciente de que deve reportar à Diretoria prontamente quaisquer violações ao presente Código; e
7. o colaborador acima identificado firma o presente Termo de Adesão de forma irrevogável e irretratável, em 2 (duas) vias, de igual teor e forma, permanecendo uma das vias arquivada na sede da VLS Legal Capital.

COLABORADOR