



CARTOR CAPITAL
GESTÃO DE RECURSOS

CÓDIGO DE ÉTICA E CONDUTA

CARTOR CAPITAL GESTÃO DE RECURSOS LTDA.
("Sociedade")

Versão vigente: Agosto/2025

CAPÍTULO I

Objetivo

1.1. Este instrumento tem por finalidade estabelecer regras e princípios que orientam a conduta dos colaboradores da Sociedade, entendendo-se como tais: (i) sócios; (ii) diretores; (iii) funcionários; (iv) estagiários; e (v) quaisquer pessoas que, em razão de seus cargos, funções ou posições na Sociedade, tenham acesso a informações confidenciais sobre a Sociedade, seus negócios ou investidores, ou que participem do processo de decisão de investimentos.

1.2. Tais princípios são de observância obrigatória por todos os colaboradores da Sociedade. Para esse fim, será coletado o Termo de Adesão e Confidencialidade, nos termos do Anexo, por meio do qual os colaboradores declaram ciência integral das regras e princípios aqui estabelecidos, previamente apresentados pelo responsável pelo Compliance da Sociedade, acerca dos quais não subsiste qualquer dúvida, comprometendo-se a cumpri-los em todas as suas atividades.

1.3. O Termo de Adesão e Confidencialidade será arquivado na sede da Sociedade, em meio físico ou digital, devendo ser coletado até o último dia do mês subsequente à contratação de novo colaborador.

1.4. O responsável pelo Compliance permanecerá à disposição para esclarecimento de dúvidas. O inteiro teor deste Código, assim como dos demais manuais e políticas internas adotadas pela Sociedade, deverá ser apresentado a todo novo colaborador no ingresso e, posteriormente, de forma periódica, conforme o Programa de Treinamento descrito abaixo.

CAPÍTULO II

Princípios Norteadores das Condutas

2.1. Todos os colaboradores da Sociedade devem (i) desempenhar suas atividades e pautar suas condutas em conformidade com os valores da boa-fé, lealdade, transparência, diligência e veracidade, evitando quaisquer práticas que possam ferir a relação fiduciária mantida com os investidores; (ii) empregar, no exercício de suas funções, o mesmo zelo que uma pessoa prudente e diligente dedica à administração dos próprios negócios, assumindo responsabilidade por quaisquer infrações ou irregularidades eventualmente cometidas; (iii) manter condutas compatíveis com os princípios de idoneidade moral e profissional.

2.2. Os esforços para a eficiência na gestão de recursos de terceiros devem ter por

objetivo proporcionar o melhor retorno aos investidores, baseando-se na análise e interpretação de informações divulgadas ao mercado, e jamais no uso de informações privilegiadas.

2.3. Os Colaboradores devem pautar sua atuação com transparência e linguagem clara. É expressamente vedada a promessa, garantia ou sugestão, ainda que indireta, de rentabilidade futura ou de ausência de riscos, sendo obrigatória a utilização de informações precisas e equilibradas em todas as comunicações, nos termos do art. 48, §2º e do art. 59 da Resolução CVM nº 175. O relacionamento dos colaboradores com participantes do mercado e formadores de opinião deve ocorrer estritamente de modo ético e transparente, evitando a adoção de qualquer prática caracterizadora de concorrência desleal e/ou condições não equitativas.

2.4. Comunicações e Material de Divulgação. Qualquer comunicação institucional, publicitária ou material de divulgação relacionado aos fundos, classes e estratégias sob gestão deve: (i) ser previamente revisada e aprovada pelo Compliance; (ii) observar linguagem precisa, equilibrada e isenta de promessa de rentabilidade ou ausência de risco; (iii) ser veiculada exclusivamente por canais oficiais definidos pela Sociedade; e (iv) manter registro de versões e aprovações internas. As informações periódicas e eventuais devem ser disponibilizadas em local de destaque e de acesso público gratuito, conforme disciplina da Resolução CVM nº 175.

2.5. Sempre que, no exercício de suas atribuições, identificarem violação à legislação ou às normas internas de conduta, os colaboradores devem comunicar o ocorrido ao Compliance.

2.6. A Sociedade transferirá às carteiras sob gestão, de forma integral, qualquer benefício ou vantagem obtidos em decorrência de sua condição de gestora profissional de recursos, vedado o auferimento de benefício pessoal em prejuízo dos fundos e de seus investidores, observadas as exceções previstas em norma específica.

2.7. Além do disposto acima, os colaboradores devem observar, no desempenho de suas atividades, os seguintes padrões de conduta:

- a) não fazer, em hipótese alguma, propaganda garantindo níveis de rentabilidade, com base em desempenho histórico da carteira ou de valores mobiliários e índices do mercado de valores mobiliários;
- b) não fazer quaisquer promessas quanto a retornos futuros;
- c) não negociar títulos e valores mobiliários com a finalidade de gerar receitas de

corretagem ou de rebate para si ou para terceiros; e

- d) não negligenciar, em qualquer circunstância, a defesa dos direitos e interesses do cliente.

Política de Soft Dollar e de Presentes

2.8. A Sociedade adota postura conservadora quanto ao Soft Dollar, permitindo sua aceitação apenas quando não houver influência sobre a independência da tomada de decisão de investimento, a escolha de parceiros, a isonomia entre investidores e/ou qualquer tipo de compromisso do colaborador em contrapartida.

2.9. É estritamente proibido o recebimento ou o oferecimento de entretenimento, presentes ou benefícios de qualquer valor a/de funcionários públicos, pessoas ou organizações, particulares ou públicas, excetuando-se os casos de pessoas ou entidades que possuam relacionamento comercial com a Sociedade e desde que em valor de até R\$ 250,00 (duzentos e cinquenta reais).

2.10. Brindes promocionais são permitidos desde que contenham a identificação do fornecedor ou cliente. Em caso de dúvida, o colaborador deve aconselhar-se com o Compliance antes da aceitação.

CAPÍTULO III

Tratamento das Informações Confidenciais

3.1. Consideram-se de natureza confidencial todas as informações a que os colaboradores tenham acesso em razão do desempenho de suas funções na Sociedade, inclusive por meio dos sistemas e arquivos disponibilizados, desde que não sejam notória e comprovadamente de domínio público.

3.2. São consideradas confidenciais ainda as informações reservadas ou privilegiadas de que trata o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, devendo ser observados para estas os mesmos princípios de conduta e controle definidos neste Código.

3.3. Assim, todos os colaboradores da Sociedade, conforme definido no item 1.1 deste Código, podem eventualmente ter acesso a informações de cunho confidencial ou privilegiado, devendo cumprir as diretrizes da Sociedade aqui previstas e nas demais políticas e manuais internos, a fim de assegurar o tratamento adequado dessas informações e prevenir o acesso por terceiros não autorizados.

3.4. Compete aos colaboradores da Sociedade:

- a) abster-se de utilizar informação privilegiada para obter, em benefício próprio ou de outrem, vantagem mediante negociação de títulos e/ou valores mobiliários;
- b) abster-se de recomendar ou de qualquer forma sugerir que qualquer pessoa compre, venda ou retenha títulos e/ou valores mobiliários se a informação a que tenha acesso privilegiado puder, em tese, influenciar a tomada de qualquer uma dessas decisões;
- c) advertir, de forma clara, àqueles em relação a quem se verificar a necessidade de revelar informação privilegiada, 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 mediante negociação com tais títulos e/ou valores mobiliários; e
- d) 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 Sociedade 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.

3.5. Considera-se informação relevante qualquer dado não divulgado ao mercado que possa influenciar a decisão de investimento de quaisquer investidores ou afetar significativamente a precificação de ativos, conforme arts. 103 e 104 da Resolução CVM nº 175. É vedado o uso ou repasse de tais informações antes de sua divulgação oficial. Tal determinação se aplica igualmente às informações obtidas/repassadas verbal ou informalmente, assim como as escritas ou impressas.

3.6. O fornecimento de informações confidenciais a pessoas externas à Sociedade será realizado somente nos casos estritamente necessários a fim de cumprir as normas atinentes à atividade desenvolvida pela Sociedade, proteção contra fraudes ou qualquer outra atividade ilegal suspeita.

3.7. Os colaboradores comprometem-se à manutenção da confidencialidade das informações que tenha acesso mediante a assinatura do Termo de Adesão e Confidencialidade. Já os terceiros contratados que tiverem acesso a informações confidenciais deverão assinar Termo de Confidencialidade específico, caso o próprio Contrato de Prestação de Serviço não possua cláusula explícita para este fim. Os

respectivos termos ficarão arquivados na Sociedade, em meio eletrônico ou físico, pelo prazo mínimo de 5 (cinco) anos.

3.8. Sob nenhuma circunstância os colaboradores poderão utilizar informações confidenciais para obter vantagens pessoais, tampouco poderão fornecê-las para terceiros, inclusive familiares, parentes e amigos, ou mesmo a outros colaboradores da Sociedade que não necessitem de tais informações para executar suas tarefas.

3.9. Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, procurar o responsável pelo Compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva e conservadora ao conceito de informação confidencial definido acima.

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

CAPÍTULO IV

Treinamento

4.1. O programa de treinamento da Sociedade, dividido em 02 (duas) etapas distintas, abrange os colaboradores e quaisquer pessoas que, em razão de seus cargos, funções ou posições na Sociedade, tenham acesso a informações confidenciais ou participem do processo de decisão de investimentos.

4.2. A primeira etapa consiste na apresentação periódica pelo Diretor de Compliance dos normativos internos ao colaborador no ato do seu ingresso na Sociedade, disponibilizando-se para prestar quaisquer esclarecimentos que se façam necessários.

4.3. Já a segunda etapa do treinamento ocorre anualmente quando o Diretor de Compliance, colaborador por ele designado, ou terceiro contratado para este fim, abordará rotinas e processos descritos nos manuais e políticas internas, dando ênfase aos casos práticos ocorridos internamente ou no mercado, que sejam de conhecimento público.

4.4. O Compliance poderá promover treinamentos em periodicidade menor caso julgue necessário, visando a atualização e ampliação do conhecimento dos colaboradores acerca de novidades normativas e regulatórias, bem como discutir casos concretos ocorridos dentro e fora da instituição.

CAPÍTULO V

Conflito de Interesse e Segregação de Atividades e Funções

5.1. Considera-se conflito de interesses qualquer interesse pessoal do Colaborador, próprio ou de terceiros, contrário ou potencialmente contrário aos interesses da Sociedade ou de seus investidores. Os Colaboradores devem atuar com diligência, lealdade e probidade, buscando as melhores condições para os fundos, evitando práticas que gerem conflitos e revertendo aos fundos quaisquer benefícios obtidos em razão da função, abstendo-se de receber vantagens que comprometam a independência, conforme art. 106 da Resolução CVM nº 175; potenciais conflitos devem ser comunicados imediatamente ao Compliance e, quando aplicável, à CVM.

5.2. É vedado receber remuneração, vantagem ou benefício, direta ou indiretamente, que possa afetar a independência na tomada de decisão ou prejudicar os interesses dos fundos. Os Colaboradores devem abster-se de atuar em qualquer processo decisório quando houver conflito de interesse real, potencial ou mesmo a sua aparência, devendo comunicar o fato ao Compliance e observar as orientações para mitigação e, se aplicável, reportar à CVM.

5.3. Os colaboradores devem evitar exercer outras funções fora da Sociedade que possam gerar conflitos de interesse, ou mesmo a sua aparência. Devem, igualmente, abster-se de defender interesses de terceiros que possam conflitar com a tomada de decisão e implicar qualquer prejuízo para a Sociedade ou seus investidores.

5.4. Caso pretenda desempenhar outras atividades, com ou sem fins lucrativos, além daquelas exercidas na Sociedade, o colaborador deverá comunicar previamente o responsável pelo Compliance para obtenção da devida aprovação, a fim de prevenir potenciais conflitos de interesse.

5.5. Caberá ao Compliance orientar a estrutura de governança da Sociedade, visando garantir a segregação de atividades no âmbito interno e evitando conflitos de interesse, ainda que potenciais, entre as atividades desenvolvidas pelos colaboradores na instituição ou empresas ligadas.

5.6. A fim de evitar potenciais conflitos de interesse no que se refere à organização funcional da Sociedade, todos os colaboradores que atuam na atividade de gestão profissional de recursos de terceiros, participando do processo de análise, seleção e tomada de decisão de investimentos, dedicam-se com exclusividade à esta atividade.

5.7. A Sociedade disponibiliza ambiente físico segregado aos seus colaboradores, assim

como infraestrutura tecnológica dedicada exclusivamente à consecução da atividade de gestão profissional de recursos de terceiros, os quais são protegidos pelos controles descritos na Política de Segurança da Informação, Segurança Cibernética e Proteção de Dados adotada pela Sociedade.

5.8. As atividades de gestão de risco e Compliance são coordenadas pelo Diretor de Risco, Compliance e PLD, podendo a equipe de risco e Compliance contar com profissionais compartilhados. Neste sentido, as atividades relacionadas à análise e gestão de riscos serão desempenhadas na forma da Política de Gestão de Riscos adotada pela Sociedade, servindo os controles internos para confirmação das ações tomadas para fins de observância da mencionada Política.

CAPÍTULO VI

Utilização dos Bens e Equipamentos

6.1. O patrimônio da Sociedade deve ser utilizado exclusivamente em consonância com seu objeto social; é dever de todos os colaboradores zelar por sua preservação e uso adequado.

6.2. Os meios de comunicação fornecidos pela Sociedade destinam-se exclusivamente a assuntos corporativos. Para fins de controle e segurança, chamadas e mensagens poderão ser monitoradas e até gravadas.

6.3. São permitidas ligações telefônicas particulares, desde que pautadas pelo bom senso; recomenda-se, prioritariamente, o uso de telefones fixos. O uso de celulares pessoais é admitido, devendo ser reduzido ao mínimo necessário.

6.4. Os recursos de acesso à internet e o serviço de correio eletrônico (e-mail) devem ser empregados apenas para assuntos corporativos; a utilização para fins particulares é excepcional e somente quando estritamente necessária. Para preservar esses recursos, a Sociedade reserva-se o direito de monitorar e controlar seus conteúdos e formas de utilização.

6.5. É permitido o uso da rede para armazenamento de arquivos pessoais, desde que a pasta esteja devidamente identificada; o colaborador está ciente de que não há garantia de privacidade sobre as informações ali armazenadas, as quais poderão ser acessadas por quaisquer colaboradores que possuam acesso à rede.

6.6. Os colaboradores não poderão utilizar os ativos da Sociedade para:

- a) visitar sites na internet que contenham materiais obscenos, lascivos, preconceituosos ou outro tipo de material repreensível;
- b) enviar ou receber material obsceno ou difamatório ou cujo objetivo seja aborrecer, assediar ou intimidar terceiros;
- c) objetivar fins ilícitos de qualquer natureza; e
- d) apresentar opiniões pessoais como se fossem da Sociedade.

CAPÍTULO VII

Política Anticorrupção

7.1. É absolutamente vedado aos colaboradores, de forma direta ou por intermédio de terceiros, praticar atos lesivos contra a administração pública, nacional ou estrangeira, que atentem contra o patrimônio público, os princípios da administração pública ou os compromissos internacionais assumidos pelo Brasil, assim definidos:

I - prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II - comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos na legislação e regulamentação que tratam da responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública (“Normas Anticorrupção”);

III - comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV - no tocante a licitações e contratos:

- a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
- b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
- c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
- d) fraudar licitação pública ou contrato dela decorrente;

- e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
- f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
- g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

V - dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do Sistema Financeiro Nacional.

7.2. É expressamente vedado ao colaborador, agindo em nome próprio ou da Sociedade, dar, oferecer, prometer, pagar ou autorizar, direta ou indiretamente, dinheiro ou qualquer coisa de valor a servidor público, autoridade governamental, consultores, representantes, parceiros ou quaisquer terceiros, com o objetivo de influenciar ato ou decisão do agente ou do governo, assegurar vantagem indevida ou direcionar negócios a qualquer pessoa, em violação às Normas Anticorrupção.

7.3. O colaborador deve estar ciente de que qualquer valor oferecido a agentes públicos, por menor que seja e independentemente de sua aceitação, pode ensejar a aplicação das penalidades previstas nas Normas Anticorrupção à Sociedade; nessa hipótese, o colaborador estará obrigado a indenizá-la por meio das medidas legais cabíveis.

7.4. Os colaboradores devem questionar a legitimidade de quaisquer pagamentos solicitados por autoridades ou agentes públicos que não possuam respaldo legal ou regulamentar.

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

7.6. A seleção de fornecedores e prestadores seguirá critérios técnicos, éticos e profissionais, com due diligence proporcional ao risco e monitoramento contínuo. É vedada a contratação ou manutenção de terceiros com histórico, indícios relevantes ou condenação por práticas corruptivas, com atenção reforçada a contrapartes

indicadas por autoridades, servidores públicos ou executivos de entes públicos, a fim de proteger a reputação da Sociedade e dos fundos.

7.7. Qualquer suspeita ou indício de práticas corruptivas por parte de colaboradores deve ser comunicada imediatamente à Diretoria.

CAPÍTULO VIII

Comunicação com a Imprensa

8.1. Para resguardar os interesses da Sociedade diante do volume de informações manejadas diariamente, somente os membros da Diretoria, ou pessoa por eles previamente e expressamente autorizada, podem manter, em nome da Sociedade, qualquer comunicação com jornalistas, repórteres, entrevistadores ou demais agentes da Imprensa.

8.2. 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.

8.3. É vedado, em qualquer circunstância, prestar declarações à Imprensa que possam aparentar ou conter conteúdo discriminatório em razão de raça, religião, cor, origem, idade, sexo, incapacidade física ou mental, ou de qualquer outra forma não autorizada expressamente em lei, bem como utilizar expressões de baixo calão ou incompatíveis com a boa educação.

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

CAPÍTULO IX

Propriedade Intelectual

9.1. A propriedade intelectual de todos os documentos, arquivos, modelos, metodologias, fórmulas, cenários, projeções, análises e relatórios produzidos no âmbito das atividades da Sociedade, ou a elas diretamente relacionados, pertence exclusivamente à Sociedade.

9.2. Ressalvada autorização expressa e por escrito do Compliance da Sociedade, a exportação, o envio a terceiros, a cópia, descrição, utilização ou adaptação fora do ambiente da Sociedade, em qualquer circunstância, de qualquer item sujeito à propriedade intelectual da Sociedade são vedadas, sujeitas à apuração de responsabilidades nas esferas cível e criminal.

9.3. Uma vez rompido o vínculo com a Sociedade, o ex-colaborador permanece obrigado a observar as restrições mencionadas acima, sujeito à responsabilização pela via judicial.

CAPÍTULO X

Procedimentos de Segurança da Informação

10.1. Acesso Restrito

10.1.1. A troca de informações entre os colaboradores da Sociedade deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de Compliance deve ser acionada previamente à revelação.

10.1.2. Os colaboradores com acesso a sistemas de informação são responsáveis por adotar as precauções necessárias para impedir acessos não autorizados, devendo resguardar senhas e demais credenciais de acesso.

10.1.3. O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

10.1.4. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela Sociedade permitem a identificação do seu remetente/receptor.

10.1.5. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se àqueles fornecidos pela Sociedade.

10.1.6. A outorga e o cancelamento de senhas são de responsabilidade da área de TI, sempre mediante orientação do Diretor de Compliance, a quem compete verificar a estrutura de governança da Sociedade para evitar transgressões às barreiras de informação e potenciais conflitos de interesse. Este procedimento também deverá ser observado em caso de mudança de atividade ou área de um profissional..

10.1.7. As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de 3 (três) tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

10.1.8. Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha ou digital que exige que a sessão somente possa ser reiniciada depois que o usuário tenha

se autenticado novamente.

10.1.9. Em caso de desligamento ou saída de colaborador, o acesso a arquivos será automaticamente bloqueado e a respectiva senha imediatamente revogada. Para sistemas externos, a Sociedade deverá submeter, de imediato, a solicitação de revogação de acesso e assegurar sua efetivação na sequência.

10.1.10. O controle de acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros da Sociedade, não sendo o espaço físico compartilhado com outras empresas ou atividades.

10.2. Backup

10.2.1. Todos os documentos arquivados nos computadores da Sociedade são objeto de backup diário na nuvem com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

10.3. Cópia de Arquivos e Instalações

10.3.1. Somente programas previamente aprovados pela área de TI podem ser utilizados pelos colaboradores. Downloads, de qualquer natureza, são permitidos desde que devidamente justificados e alinhados aos objetivos e às necessidades da Sociedade.

10.3.2. A cópia de arquivos e a instalação de programas em equipamentos da Sociedade devem observar integralmente os direitos de propriedade intelectual aplicáveis (como licenças e patentes), sendo proibido o uso de softwares não licenciados ou não autênticos.

10.3.3. É expressamente proibido que colaboradores façam cópias (físicas ou eletrônicas) ou imprimam arquivos utilizados, gerados ou disponíveis na rede e circulem com esses arquivos em ambientes externos, salvo quando necessário para a execução e o desenvolvimento dos negócios e dos interesses da Sociedade. Nessas hipóteses, o colaborador que detiver a posse e a guarda do arquivo será o responsável direto por sua adequada conservação, integridade e pela manutenção de sua confidencialidade.

10.3.4. Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Sociedade. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

10.4. Descarte de Informações

10.4.1. As seguintes diretrizes devem ser observadas no descarte de informações:

(i) o conteúdo descartado deverá ser apagado 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 imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;

(iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada.

(iv) devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável, os dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade.

10.5. Redundância

10.5.1. Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe poderá acessar as informações na nuvem de qualquer local.

10.5.2. Para assegurar a continuidade da rede e a integridade dos dados, inclusive em eventuais interrupções no fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a nobreaks, garantindo operação por tempo suficiente para que os usuários salvem seus arquivos.

10.6. Suporte e Monitoramento

10.6.1. Em caso de indisponibilidade da rede ou de alguma estação de trabalho, a área de TI deve ser comunicada imediatamente, providenciando o suporte interno ou acionando o suporte externo necessário.

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

10.6.3. Considerando que o e-mail é destinado exclusivamente a fins profissionais e ao desempenho das atividades dos colaboradores, a Sociedade poderá monitorar

integralmente as trocas de mensagens, internas e externas, realizadas pelos colaboradores

10.6.4. Qualquer suspeita ou ciência de violação desta Política ou incidente de segurança da informação deve ser prontamente reportada ao Compliance, para imediata apuração dos fatos, mitigação de riscos, implementação de medidas corretivas e responsabilização dos envolvidos.

10.6.5. Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

10.7. Tratamento de casos de vazamento de informações confidenciais

10.7.1. Em caso de vazamento de informações confidenciais relacionadas a investidores, ou de qualquer Dado Pessoal ou Dado Pessoal Sensível tratado pela Sociedade, ainda que decorrente de ação involuntária, o Diretor de Compliance notificará os interessados. Tratando-se de Dado Pessoal ou Dado Pessoal Sensível, a Autoridade Nacional de Proteção de Dados (ANPD) e o titular do dado também serão comunicados, conforme os parâmetros da Lei Geral de Proteção de Dados.

10.7.2. Sem prejuízo, a Sociedade acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

10.7.3. Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

10.8. Firewall

10.8.1. A Sociedade faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas.

10.9. Testes de Segurança

10.9.1. São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real

Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Monitoramento de Hosts e serviços	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 15 min
Back Online	Tempo real
Backup Firewall	A cada alteração
Documentação	A cada mudança
Verificar sistema gráficos de consumo de link, visão diária, semanal e mensal	Mensal
Troca da senha dos usuários	Trimestral

CAPÍTULO XI

Tratamento de Dados Pessoais

11.1. A Sociedade assegura a observância, a implementação e o cumprimento das regras, políticas e procedimentos de Segurança da Informação, conforme o capítulo anterior, bem como de Segurança Cibernética, nos termos da Política de Segurança Cibernética e Proteção de Dados.

11.2. Sem prejuízo das diretrizes deste Código e com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, a Sociedade adota regras e procedimentos para o tratamento de dados pessoais e, quando aplicável, de dados pessoais sensíveis, inclusive em meios digitais, em conformidade com a Lei Geral de Proteção de Dados. Para os fins deste Código, entende-se por:

“Dados Pessoais”: qualquer informação relacionada a pessoa natural identificada ou identificável.

“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.

11.3. Todos os Dados Pessoais ou Dados Pessoais Sensíveis são informações confidenciais e devem ser tratados como tal para os fins deste Código e demais manuais e políticas internas adotadas pela Sociedade.

CAPÍTULO XII

Disposições Gerais e Enforcement

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

12.2. Sem prejuízo de outras vedações estabelecidas na Resolução CVM nº 175 e respectivos Anexos, são vedados: (i) prometer rentabilidade ou ausência de risco; (ii) contrair empréstimos em nome dos fundos, salvo se expressamente previsto no regulamento; (iii) vender cotas a prazo; (iv) praticar atos que gerem benefício pessoal em prejuízo do fundo; (v) utilizar ativos do fundo para benefício próprio ou de terceiro.

12.3. A título de *enforcement*, vale notar que a não observância deste Código sujeitará o infrator a medidas disciplinares, que podem incluir advertência, suspensão e demissão/exclusão por justa causa, conforme a gravidade e reincidência, sem prejuízo das responsabilidades civis, criminais e, quando aplicável, da comunicação às autoridades competentes.

12.4. Este Código será revisado anualmente, sendo mantido o controle de versões. A cada revisão será coletado novo Termo de Adesão e Confidencialidade dos colaboradores, na forma e para fins de atendimento aos itens 1.2 e 1.3. do presente.

12.5. A Sociedade e seus Colaboradores zelarão para que as informações periódicas e eventuais dos fundos sejam tempestivamente disponibilizadas nos canais oficiais, em local de destaque e de acesso gratuito, observando a disciplina aplicável da Resolução CVM nº 175.

TERMO DE ADESÃO E CONFIDENCIALIDADE

Pelo presente Termo de Adesão e Confidencialidade, [NOME], [nacionalidade], [profissão], portador da carteira de identidade nº [definir], expedida pelo [órgão expedidor], inscrito no CPF sob o nº [definir], na qualidade de colaborador da **CARTOR CAPITAL GESTÃO DE RECURSOS LTDA.** (“Sociedade”), declaro que:

- a) recebi cópia dos manuais e políticas identificados no quadro infra, tendo sido apresentado o seu teor pelo Diretor de Compliance, o qual colocou-se à disposição para esclarecer toda e qualquer dúvida porventura existente;
- b) compreendi a integralidade dos termos e disposições definidos pelos manuais e políticas em questão, comprometendo-me a cumpri-los e observá-los no dia-a-dia das minhas atividades.

Manual/Política	Adesão X [OU] N/A
Código de Ética e Conduta	
Manual de Compliance	
Política de Gestão de Riscos	
Política de Investimentos Pessoais	
Política de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo	
Política de Seleção, Contratação e Monitoramento de Prestadores de Serviços	
Plano de Continuidade de Negócios	
Política de Segurança Cibernética e Proteção de Dados	
Política de Rateio e Divisão de Ordens	

Comprometo-me a observar todas as regras, manuais e políticas internas definidas pela Sociedade, legislação e regulamentação aplicáveis às minhas atividades e às atividades da Sociedade, e estou ciente de que a não observação dessas regras poderá caracterizar falta grave, passível de punição, inclusive rescisão contratual ou de exclusão por justa causa do quadro societário.

Comprometo-me a informar ao Diretor de Compliance quaisquer violações ou indícios de violação a que tenha ciência às regras internas definidas pela Sociedade, assim como à legislação e regulamentação aplicáveis à minha atividade e às atividades da Sociedade.

Autorizo o Compliance ao tratamento dos meus dados pessoais, sensíveis ou não, para

fins de cumprimento das leis e normas que regem a atividade da Sociedade, 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, não afetando, entretanto, a legalidade de nenhum tratamento realizado em momento anterior à revogação, bem como o tratamento lícito dispensado da necessidade de consentimento.

Declaro ciência que, durante o exercício das minhas atividades profissionais na Sociedade, poderei ter acesso a informações confidenciais, conforme definido no Código de Ética e Conduta. Na qualidade de colaborador e mesmo após o término do vínculo com a Sociedade, comprometo-me a guardar sigilo em relação às Informações Confidenciais, sendo expressamente vedada sua revelação a terceiros ou a colaboradores não autorizados da Sociedade ou sua utilização para outros fins que não a devida execução das minhas atividades profissionais na Sociedade.

Dessa maneira e por meio deste Termo, comprometo-me a zelar para que Informações Confidenciais permaneçam restritas ao conhecimento de colaboradores autorizados ou que necessitem dessas informações para a devida execução de suas atividades profissionais na Sociedade.

Declaro, ademais, que informarei ao Compliance caso eu seja considerado Pessoa Politicamente Exposta (“PPE”), ou caso possua relacionamento ou ligação com PPE.

Declaro, ainda, que:

- a. Possuo reputação ilibada;
- b. Nunca estive inabilitado(a) ou suspenso(a) para o exercício de cargo em instituições financeiras e demais entidades autorizadas a funcionar pela CVM, pelo Bacen, pela SUSEP ou pela PREVIC;
- c. Nunca fui condenado(a) por crime falimentar, prevaricação, suborno, concussão, peculato, lavagem de dinheiro ou ocultação de bens, direitos e valores, contra a economia popular, a ordem econômica, as relações de consumo, a fé pública ou a propriedade pública, o sistema financeiro nacional, ou a pena criminal que vede, ainda que temporariamente, o acesso a cargos públicos, por decisão transitada em julgado, ressalvada a hipótese de reabilitação;
- d. Não estou impedido(a) de administrar seus bens ou deles dispor em razão de decisão judicial ou administrativa;

Nunca sofri punição definitiva, nos últimos 05 (cinco) anos, em decorrência da minha atuação como administrador ou membro do conselho fiscal de entidade sujeita ao controle e fiscalização dos órgãos reguladores mencionados acima.

Por fim, declaro que mantereirei o Compliance atualizado sobre quaisquer mudanças nas informações prestadas neste Termo.

O presente Termo de Adesão e Confidencialidade é firmado, de forma irrevogável e irretratável, em 2 (duas) vias, de igual teor e forma, permanecendo uma das vias arquivada na sede da Sociedade.

Belo Horizonte, de de

COLABORADOR: