

CÓDIGO DE ÉTICA E CONDUTA
FRS CONSULTORIA PATRIMONIAL E DE INVESTIMENTOS LTDA.
("Sociedade")

Versão vigente: Fevereiro/2021
Versão anterior: novembro/2020

1. Objetivo

1.1. O Código de Ética e Conduta ("Código") tem como objetivo precípuo a definição de regras e princípios norteadores das condutas dos colaboradores da Sociedade, assim entendidos seus sócios, funcionários, diretores, estagiários ou quaisquer outras pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações relevantes e confidenciais sobre a Sociedade, seus negócios ou clientes ("Colaboradores", no plural, ou "Colaborador", no singular).

1.2. Tais princípios deverão ser compulsoriamente observados pelos Colaboradores da Sociedade, declarando estarem cientes de todas as regras e políticas aqui expostas, que lhes foram previamente apresentadas pelo responsável pelo Compliance da Sociedade e em relação às quais não existe qualquer dúvida, comprometendo-se a observá-las a todo tempo no desempenho de suas atividades, conforme Termo de Adesão e Confidencialidade constantes do Anexo I ao presente Código.

1.3. O Termo de Adesão e Confidencialidade deve ser coletado até o último dia do mês subsequente à contratação de novo colaborador e, ainda, quando da alteração de qualquer Política da Sociedade, sendo arquivado na sede da Sociedade em meio físico ou digital.

1.4. Em caso de dúvidas a respeito das disposições aqui contidas, o Colaborador deve consultar o Diretor responsável pelo Compliance ("Diretor de Compliance").

2. Princípios Norteadores das Condutas

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

2.2. Todos os Colaboradores da Sociedade deverão agir com probidade, pautando suas condutas em conformidade com os valores da boa-fé e ética profissional, de forma a empregar no exercício de suas atividades todo o cuidado e diligência esperados de um profissional em sua posição, em relação aos clientes, evitando quaisquer práticas que possam ferir a relação fiduciária mantida

com os clientes.

2.3. Todos os esforços em prol da eficiência da atividade de consultoria de valores mobiliários devem visar à obtenção de melhor retorno aos clientes e colocando os interesses dos clientes acima dos da Sociedade e dos próprios Colaboradores, com base na análise e interpretação de informações divulgadas ao mercado, e jamais no acesso a informações privilegiadas.

2.4. Os Colaboradores deverão observar as regras e procedimentos internos relacionados a forma e prazos de arquivamento de toda documentação relacionada ao processo de cadastro e Suitability de clientes, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, cálculos que fundamentaram a cobrança de taxa de performance de clientes classificados como investidores profissionais, relatórios e pareceres relacionados com o exercício de suas atividades e os estudos e análises que fundamentaram as orientações, recomendações ou aconselhamentos, conforme orientações do departamento de Compliance.

2.5. A Sociedade transferirá aos clientes qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de consultora de valores mobiliários, observadas as exceções previstas em normas específicas.

2.6. Sem prejuízo do acima estabelecido, é vedado à Sociedade e aos Colaboradores:

- a) atuar na estruturação, originação e distribuição de produtos que sejam objeto de orientação, recomendação e aconselhamento aos clientes, salvo se observadas as normas sobre segregação de atividades;
- b) proceder a qualquer tipo de modificação relevante nas características básicas dos serviços prestados, exceto quando houver autorização, prévia e por escrito, do cliente;
- c) fazer propaganda garantindo níveis de rentabilidade, com base em desempenho histórico de valores mobiliários e índices de mercado de valores mobiliários;
- d) fazer promessas quanto a retornos futuros;
- e) omitir informações sobre eventuais conflitos de interesses e riscos relativos ao objeto da consultoria prestada;
- f) receber qualquer remuneração, benefício ou vantagem, direta ou indiretamente por meio de partes relacionadas, que potencialmente prejudique a independência na prestação de serviço de consultoria de valores mobiliários a clientes que não sejam considerados investidores profissionais e, conseqüentemente, não tenham assinado Termo de Ciência de potencial conflito de interesses; e

- g) atuar como procurador ou representante de seus clientes perante instituições integrantes do sistema de distribuição de valores mobiliários, para fins de implementar e executar as operações que reflitam as recomendações objeto da sua prestação de serviço.

2.7. Os Colaboradores da Sociedade devem estar conscientes de que a informação transparente, precisa e oportuna constitui o principal instrumento à disposição do público investidor, para que lhes seja assegurado o indispensável tratamento equitativo. As informações prestadas ao investidor não devem, de forma efetiva ou aparente, assegurar a existência de resultados futuros ou a isenção de riscos.

2.8. O relacionamento dos Colaboradores da Sociedade com os participantes do mercado e com os formadores de opinião deve dar-se de modo ético e transparente, evitando a adoção de qualquer prática caracterizadora de concorrência desleal e/ou condições não equitativas

2.9. Os Colaboradores deverão informar ao Diretor de Compliance sempre que se verifique, no exercício de suas atribuições, a ocorrência de violação à legislação ou às normas internas de conduta.

3. Tratamento das Informações e sua Classificação

3.1. Consideram-se informações de natureza confidencial todas as informações às quais os colaboradores venham a ter acesso em decorrência do desempenho de suas funções na Sociedade, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto, que não sejam notória e comprovadamente de domínio público.

3.2. Os Colaboradores da Sociedade deverão:

- a) abster-se de utilizar informação privilegiada para obter, em benefício próprio ou de outrem, vantagem mediante recomendação com tais 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 recomendação com tais títulos e/ou valores mobiliários, inclusive mediante a coleta de Termo de Confidencialidade, se for o caso; 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.

3.3. Os Colaboradores deverão guardar absoluto sigilo sobre toda e qualquer informação a que tenham acesso ou conhecimento no desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto. Tal determinação se aplica igualmente às informações obtidas/repassadas verbal ou informalmente, assim como as escritas ou impressas.

3.4. O fornecimento de informações não públicas 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.

3.5. 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 para este fim. Os respectivos Termos ficarão arquivados na Sociedade, em meio eletrônico, pelo prazo mínimo de 5 (cinco) anos.

3.6. 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.

3.7. Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o Colaborador deve, previamente à sua divulgação, procurar o Diretor de Compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva ao conceito informação confidencial definido acima.

3.8. A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada ao Diretor de Compliance para que seja decidida a forma mais adequada para tal revelação.

3.9. A manutenção da confidencialidade das informações às quais os Colaboradores tiverem acesso deve perdurar durante toda a existência da Sociedade, bem como após o desligamento dos Colaboradores.

4. Tratamento de Conflitos de Interesse e Segregação de Atividades e Funções

4.1. Consideram-se conflitos de interesse, de forma genérica e não limitadamente, quaisquer interesses pessoais dos Colaboradores, em benefício próprio ou de terceiros, contrários ou potencialmente contrários aos interesses da Sociedade ou dos seus clientes.

4.2. Os Colaboradores da Sociedade devem evitar desempenhar outras funções fora da Sociedade que possam gerar conflitos de interesse, ou mesmo aparentar tais conflitos. Também devem evitar defender interesses de terceiros que possam gerar conflitos de interesse na hora da recomendação de investimentos e implicar em algum tipo de prejuízo para a Sociedade ou seus clientes.

4.3. Caso o Colaborador resolva exercer outras atividades, sejam elas com ou sem fins lucrativos, além da praticada junto à Sociedade, deve comunicar previamente ao Diretor de Compliance para a devida aprovação a fim de evitar potenciais conflitos de interesse.

4.4. 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

4.5. Caso o Colaborador esteja diante de uma situação de conflito de interesses, deverá informar ao cliente o potencial conflito de interesses e as fontes desse conflito, antes de efetuar uma recomendação de investimento, bem como comunicar o Diretor de Compliance sobre o fato.

4.6. Caso o conflito de interesse, mesmo que potencial, surja após a celebração de contrato com o cliente, o Colaborador deverá informar imediatamente o Diretor de Compliance, para que as ações visando a mitigação do conflito sejam implementadas, bem como deverá notificar por e-mail ou por escrito o cliente sobre o potencial conflito e as suas fontes em até 3 (três) dias úteis depois que verificar a existência do potencial conflito.

4.7. É estritamente proibido o recebimento ou o oferecimento de entretenimento, presentes ou benefícios de qualquer valor a/de clientes, excetuando-se os casos de pessoas ou entidades que possuam relacionamento comercial com a Sociedade e desde que em valor de até R\$ 200,00 (duzentos reais), à exceção do recebimento ou oferecimento de entretenimento, presentes ou benefícios de qualquer valor a/de agente público, ocasião em que o valor máximo será de R\$ 100,00 (cem reais).

4.8. Independente do valor, não é permitido:

a) agir em troca do presente ou entretenimento;

- b) aceitar ou dar dinheiro ou equivalente (cheques, vale-presente conversível em dinheiro, títulos mobiliários ou empréstimos).
- c) aceitar ou dar um presente ou entretenimento que viole qualquer lei ou regulamentação ou que venha a denegrir a reputação da Sociedade;
- d) aceitar ou dar qualquer coisa que possa vir a ser interpretada como suborno ou influência indevida;
- e) aceitar ou dar presente ou entretenimento que viole os padrões de conduta da Sociedade;
- f) fazer uso de sua posição, de qualquer maneira, para obter algo de valor de clientes, estabelecidos ou potenciais, ou de pessoas com as quais tenha relações de negócios;
- g) fornecer entretenimento que seja excessivamente luxuoso ou frequente para clientes, estabelecidos ou potenciais;
- h) participar de qualquer entretenimento que seja inapropriado, de conteúdo sexual ou inconsistente com práticas empresariais éticas;
- i) aceitar presentes ou entretenimento ou dar presentes ou entretenimento a qualquer fornecedor/prestador de serviço durante o processo de seleção ou concorrência;
- j) participar de qualquer ação que leve outra pessoa a violar os padrões de sua própria companhia quanto a presentes e entretenimento;
- k) dar presente ou entretenimento as clientes, estabelecidos ou potenciais, que não seja adequadamente anotado nos livros e registros da Sociedade.

4.8. Nenhum cliente deve ter tratamento privilegiado em detrimento de outro, por qualquer razão, devendo o relacionamento com todos os clientes ser objetivo e equânime.

5. Proteção de Dados Pessoais

5.1. O presente tópico visa regulamentar o tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Sociedade, 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.

5.2. Considera-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, clientes, parceiros, prestadores de serviço ou quaisquer terceiros com os quais a Sociedade mantenha relacionamento de qualquer natureza.

5.2.1. São considerados, ainda, Dados Pessoais aqueles utilizados para formação de perfil comportamental de determinada pessoa natural, se identificada.

5.3. 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.

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

5.5. 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 Sociedade, 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.

5.6. O tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Sociedade só será realizado nas seguintes hipóteses:

- (i) para o cumprimento de obrigação legal ou regulatória pela Sociedade;
- (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 Sociedade ou de terceiros, 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.

5.6.1. O legítimo interesse da Sociedade indicado no item 5.6. (iii) acima poderá ter fundamento, mas não se limita, às seguintes finalidades:

- (i) apoio e promoção de atividades da Sociedade; 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.

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

5.6.2. O consentimento de que trata o item 5.6 (iv) 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.

5.7. A Sociedade 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 consultoria em valores mobiliários em virtude de obrigação regulatória;

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

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

(iv) informações acerca do potencial compartilhamento de dados pela Sociedade 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.

5.8. 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.

5.9. 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 pela Sociedade;

(ii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos acima; ou

(iii) uso exclusivo da Sociedade, vedado seu acesso por terceiro, e desde que anonimizados os dados.

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

5.11. A Autoridade Nacional de Proteção de Dados poderá determinar que a Sociedade 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 Sociedade sobre estas medidas, salvaguardas e mecanismos de mitigação de risco adotados.

5.12. O encarregado pelo tratamento de Dados Pessoais e Dados Pessoais Sensíveis será o Diretor de Compliance da Sociedade. As informações para contato do encarregado estarão disponíveis no site da Sociedade.

6. Política de Segurança da Informação

6.1. Os Colaboradores da Sociedade 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.

6.2. Neste sentido, todos os Colaboradores:

a) devem manusear a informação protegida de forma apropriada, sendo vedado o acesso a informações protegidas por meio de rede não protegida;

b) são responsáveis por suas ações associadas ao uso que fazem da informação protegida;

- c) são responsáveis por reportar ao Diretor de Compliance qualquer suspeita ou conhecimento de violação desta Política de Segurança da Informação ou incidente de segurança da informação, incluindo eventual vazamento de informações de clientes ou de Colaboradores;
- d) são responsáveis por assegurar que conhecem e cumprem as políticas, as normas e as diretrizes aplicáveis às suas responsabilidades.

6.3. No que se refere ao transporte de informações protegidas, assim consideradas aquelas que não estão disponíveis ao público em geral, seja em meio físico ou meio eletrônico portátil, deve obedecer aos seguintes padrões:

- (i) a informação deve estar sempre de posse do Colaborador. Em caso de necessidade de afastamento temporário, a informação deverá ser mantida em ambiente seguro, devidamente isolado do acesso ao público;
- (ii) a informação protegida transmitida via rede não protegida (por exemplo, a internet), ou transportada em mídias portáteis, deve ser criptografada, sendo utilizado protocolo seguro como SFTP ou outro que a Sociedade entenda conveniente.

6.4. O armazenamento ou transporte de informação protegida por terceiros contratados deve observar as condições aqui definidas.

6.5. Todos os computadores ou dispositivos eletrônicos móveis disponibilizados pela Sociedade possuem senhas de acesso individuais e intransferíveis, fornecidas aos usuários pelo responsável pelo TI, 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 Sociedade permitem a identificação do seu remetente/receptor.

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

6.7. As contas de usuário, assim como as senhas de acesso, não podem ser compartilhadas por mais de um usuário. Da mesma forma, um mesmo usuário não poderá receber uma gama de autorizações que, se realizadas em conjunto, permitam que o usuário cometa fraude ou explore controles técnicos ou que configure conflito de interesses. Para o fornecimento de senhas indicado no item acima, o responsável pelo TI deve obter orientação do Diretor de Compliance, que deverá avaliar potenciais conflitos previamente à disponibilização do acesso e a quem compete a verificação da estrutura de governança da Sociedade.

6.8. A solicitação de acesso pelos usuários deve ocorrer mediante envio de e-mail ao

departamento de Compliance. Se houver uma alteração de função/responsabilidade de um usuário, os seus acessos à informação protegida devem ser revistos em até 24 (vinte e quatro) horas para assegurar que o acesso seja restrito aos ativos de informação necessários para a nova função.

6.9. As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação. As senhas não poderão ser reutilizadas por 03 (três) alterações consecutivas.

6.10. Os identificadores e os autenticadores que não sejam mais necessários, inclusive em virtude de desligamento do usuário, devem ser imediatamente revogados. Para sistemas externos, a Sociedade deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar - se de que os acessos sejam revogados.

6.11. Sem prejuízo das condições definidas acima para a identificação do usuário e consequente proteção das informações, a Sociedade observará os seguintes padrões de segurança:

- a) informação que identifique uma pessoa (como datas de nascimento, número de identidade/seguridade social, nomes, endereços) não pode ser usada como um identificador de usuário ou autenticador.
- b) sistemas internos devem permitir que os usuários mudem suas próprias senhas e essas senhas devem ser trocadas dentro de um prazo máximo de 48 (quarenta e oito) horas.
- c) quando um usuário se autentica em um sistema, o autenticador deve ser informado em um campo protegido, não legível.
- d) as mensagens de falha de autenticação devem ser genéricas e não devem descrever a razão para a falha.
- e) senhas usadas para autenticação em sistemas operacionais (como Windows ou UNIX) devem ser validadas para complexidade apropriada.
- f) sempre que um autenticador inicial de usuário é criado, ele deve expirar uma vez que ocorra a autenticação inicial bem-sucedida.
- g) senhas ou PINs devem ser reinicializados somente depois que o proprietário da conta tenha sido identificado positivamente.
- h) após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela

Sociedade expiram, usando um protetor de tela protegido por senha que exija que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

- i) se aplicativos com interface web que permitam acesso externo forem usados para processar informação protegida, duplo-fator de autenticação deve ser implementado para acesso externo.
- j) um usuário não pode ser autenticado simultaneamente em múltiplas sessões de um aplicativo.

6.12. A base de dados eletrônicos utilizada pela Sociedade é segregada de modo que informações confidenciais são arquivadas em pastas de acesso restrito, através da utilização de senha, as pessoas previamente autorizadas. O controle do acesso a arquivos e informações não públicas em meio físico é garantido através da segregação física. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se aqueles fornecidos pela Sociedade.

6.13. A troca de informações entre os Colaboradores 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 o Diretor de Compliance deve ser acionado previamente à revelação.

6.14. Todos os documentos arquivados nos computadores da Sociedade são objeto de backup 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 realizados testes de recuperação de backup no mínimo semestralmente.

6.14.1. O backup 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.

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

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

6.15. O sistema eletrônico utilizado pela Sociedade é protegido por firewall e contam com software anti-malware, devidamente atualizados, sendo capazes de interceptar, analisar e/ou controlar

acesso de escrita de arquivo sob demanda ou execução de programa, sendo realizadas verificações regulares a fim de identificar a presença de malware persistente.

6.16. O sistema eletrônico 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.

6.17. Todos os programas de computador utilizados pelos Colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática. *Downloads* e alterações de software ou configurações dos dispositivos da Sociedade só podem ser realizados mediante autorização prévia. Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de *downloads* impróprios, não autorizados ou gravados em locais indevidos.

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

6.19. É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o Colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

6.20. A informação protegida não pode ser removida das instalações da Sociedade ou enviada para ambiente externo sem a autorização do departamento de Compliance. As mídias e documentos transportados que contenham informação protegida devem ser rastreados, sendo obtida a confirmação de que foram recebidos no destino pretendido.

6.21. 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.

6.22. O descarte de informações confidenciais deve observar as seguintes diretrizes:

- a) 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;
- b) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;

- c) a eliminação ou a destruição final das mídias ou dos documentos, realizada por terceiros, que contenham informação protegida deve ser documentada.
- d) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecoverável.

6.23. 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, será possível acessar as informações na nuvem de qualquer local.

6.24. Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do estilo *no-break*, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuário salvem seus arquivos.

6.25. A Sociedade se reserva ao direito de revisar e monitorar continuamente 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 ou permissão, gravar qualquer ligação telefônica dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela Sociedade, de forma a detectar qualquer irregularidade na transferência de informações seja interna ou externamente.

6.26. 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 Sociedade também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores.

6.27. Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Diretor de Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

6.28. No caso de vazamento de informações confidenciais relacionadas aos clientes da Sociedade, ou de qualquer outro Dado Pessoal ou Dado Pessoal Sensível tratado pela Sociedade, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os interessados sobre o ocorrido. Em se tratando de Dado Pessoal ou Dado Pessoal Sensível, a Autoridade Nacional de Proteção de Dados também deverá ser comunicada, além do titular do dado. Esta comunicação observará os parâmetros exigidos pela Lei Geral de Proteção de Dados.

6.29. 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.

6.30. 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.

6.31. Para fins de segurança da informação, são realizados os seguintes testes para monitoramento dos sistemas utilizados pela Sociedade:

| 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 |
| Autenticação de rede | Tempo real |
| Bloqueio de tela do Windows por Inatividade | A cada 10 minutos |
| Backup Online | Diário |
| Atualizações nas estações de trabalho | Mensal |
| Troca da senha dos usuários | Trimestre |

6.32. A evidência dos testes acima é arquivada na Sociedade, meio eletrônico.

7. Utilização dos Bens e Equipamentos

7.1. A utilização dos ativos e sistemas da Sociedade, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

7.2. E-mails ou quaisquer outras modalidades de sistemas de comunicação devem ser utilizadas somente para os negócios da Sociedade, sendo a utilização para fins particulares tratadas como exceção. Arquivos criados nestes sistemas estão sujeitos a revisões e inspeções internas e externas.

7.3. O uso da rede para armazenar os arquivos pessoais é permitido, desde que a pasta seja corretamente identificada, ficando o Colaborador ciente de que não será assegurada privacidade às informações armazenadas, as quais poderão ser acessadas por quaisquer Colaboradores que possuam acesso à rede.

7.4. A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, cor, raça, religião, classe social, opinião política, idade, sexo, preferencial sexual, condição ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

7.5. O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Sociedade.

8. Programa de Treinamento

8.1. A Sociedade conta com um programa de treinamento dos Colaboradores da Sociedade que tenham acesso a informações confidenciais e participem do processo de recomendação de investimento dividido em 02 (duas) etapas distintas. A primeira etapa consiste na apresentação pelo responsável pelo Compliance ou colaborador por ele designado ou terceiro contratado para este fim dos normativos internos ao Colaborador no ato do seu ingresso na Sociedade e, a segunda, mediante treinamento anual da equipe sobre os procedimentos, rotinas e controles internos descritos nos manuais internos, dando ênfase aos casos práticos ocorridos internamente ou no mercado.

8.2. O departamento de Compliance poderá promover treinamentos em periodicidade menor, visando à atualização e ampliação do conhecimento dos Colaboradores acerca de novidades normativas e regulatórias, bem como discutir casos concretos ocorridos dentro e fora da instituição.

9. Política Anticorrupção

9.1. 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, 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.

9.2. É terminantemente proibido ao Colaborador agindo em seu nome ou em nome da Sociedade, 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.

9.3. A Sociedade 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.

9.4. 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 Sociedade, hipótese em que o colaborador estará sujeito a indenizar a Sociedade, por meio das medidas legais cabíveis.

9.5. 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 Sociedade são vedados.

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

9.7. A Sociedade e seus Colaboradores devem ainda verificar constantemente se terceiros prestadores de serviços e parceiros comerciais estão sendo processados ou já foram condenados por práticas corruptivas, devendo abster-se de manter relacionamento ou contratar terceiros se houver sérios indícios ou condenação em casos de corrupção ativa ou passiva. Esta previsão se aplica especialmente para contrapartes que tenham sido recomendadas à Sociedade por quaisquer autoridades, servidores públicos, funcionários ou executivos de empresas ou órgãos públicos.

9.8. Qualquer suspeita ou indício de práticas corruptivas envolvendo os Colaboradores da Sociedade ou prestadores de serviço atuando em seu nome deve ser comunicada imediatamente aos Diretores da Sociedade.

10. Propriedade Intelectual

10.1. Todos os documentos, arquivos, modelos, metodologias, fórmulas, cenários, projeções, análises e relatórios produzidos e desenvolvidos na realização das atividades da Sociedade ou a elas diretamente relacionadas, têm sua propriedade intelectual atribuída à Sociedade.

10.2. Ressalvada autorização expressa e por escrito da responsável pelo 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.

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

11. Disposições Gerais e Enforcement

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

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

11.3. 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 ao item 1.2 deste Código.

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 **FRS CONSULTORIA PATRIMONIAL E DE INVESTIMENTOS LTDA.** (“Sociedade”), declaro que:

- a) recebi cópia dos manuais e políticas identificados no quadro infra, tendo sido apresentado o seu teor pelo responsável pelo 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 Investimentos Pessoais | |
| Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo | |
| Política de Seleção, Monitoramento e Contratação de Prestadores de Serviços | |
| Plano de Continuidade de Negócios | |
| Política de Suitability | |

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 responsável pelo 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 a Sociedade 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 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.

Autorizo, ainda, o Diretor de Compliance da Sociedade e os colaboradores por ele designados para tal, conforme o caso, a realizar verificações ou pesquisas independentes utilizando meu nome e documentos, com base em informações disponíveis publicamente.

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 meus bens ou deles dispor em razão de decisão judicial ou administrativa;
- e. 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.

Rio de Janeiro, [dia] de [mês] de [ano]

[ASSINATURA DO COLABORADOR]