ETRNTY CAPITAL GESTORA DE RECURSOS LTDA.

Política de Controles Internos

Dezembro / 2023

Capítulo I – Objetivo e Abrangência

Esta política tem por objetivo estabelecer regras e procedimentos a serem observados para o fortalecimento e funcionamento dos sistemas de controles internos da Etrnty Capital Gestora de Recursos Ltda. ("Etrnty" ou "Sociedade").

Adicionalmente, essas regras e procedimentos visam garantir o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional.

Desta forma, esses procedimentos visam mitigar os riscos de acordo com a natureza, complexidade e risco das operações realizadas pela Etrnty, bem como, disseminar a cultura de controles para garantir o cumprimento da Resolução CVM 21, bem como das demais normas estabelecidas pelos órgãos reguladores e autorreguladores.

Esta Política aplica-se a todos os integrantes da Etrnty incluindo, mas não se limitando, a administradores, sócios, empregados, representantes e prestadores de serviço ("Integrantes").

Capítulo II – Base Legal

Todos os Integrantes devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Sociedade bem como do completo conteúdo deste Manual. São as principais normas aplicáveis às atividades da Etrnty:

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21");
(ii) Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM 50");
(iii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175") e seus Anexos Normativos;
(iv) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("Anbima") de Ética ("Código Anbima de Ética");
(v) Código de Administração e Gestão de Recursos de Terceiros ("Código de AGRT");
(vi) Regras e Procedimentos do Código de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III;
(vii) Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, , de 11 de julho de 2022, conforme alterada ("Normas de Anticorrupção");
(viii) Lei 9.613, de 03 de março de 1998, conforme alterada; e

(ix) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Etrnty.

I. Interpretação e Aplicação

Para fins de interpretação dos dispositivos previstos nesta Política, exceto se expressamente disposto de forma contrária: (a) os termos utilizados nesta Política terão o significado atribuído na Resolução CVM 175; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; (c) as referências a regulamento abrangem os anexos e apêndices, se houver, observado o disposto na Resolução CVM 175; e (d) as referências às Classes abrangem os Fundos ainda não adaptados à Resolução CVM 175.

As disposições da Política são aplicáveis aos Fundos constituídos após o início da vigência da Resolução CVM 175 e aos Fundos constituídos previamente a esta data que já tenham sido adaptados às regras da referida Resolução. Com relação aos Fundos constituídos antes da entrada em vigor da Resolução CVM 175, a Etrnty e os Fundos permanecerão observando as regras da Instrução CVM nº 555, de 17 de dezembro de 2014, conforme alterada ("Instrução CVM 555"), e de outras instruções aplicáveis às diferentes categorias de Fundos sob gestão, especialmente, no que diz respeito às responsabilidades e atribuições da Etrnty, enquanto gestora da carteira dos Fundos, até a data em que tais Fundos estejam adaptados às disposições da Resolução CVM 175.

Capítulo III – Dos Princípios

As atividades de controle devem ser constantemente avaliadas, tomando como referência as boas práticas de Governança Corporativa.

Os Controles Internos consistem em um processo desenvolvido para garantir que sejam atingidos os objetivos da instituição, nas seguintes categorias:

i. Eficiência e efetividade operacional;
ii. Confiança nos registros de dados e informações;
iii. Conformidade; e
iv. Abordagem baseada em risco.

Capítulo IV – Das Diretrizes

Esta Política tem como diretrizes:

i. Disseminar a cultura sobre a importância dos controles internos a todos os Integrantes da Etrnty;
ii. Assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;
iii. Alinhar a estrutura dos controles internos aos riscos e objetivos do negócio;
iv. Garantir a existência de atribuição de responsabilidades e delegação de autoridade, observada a estrutura hierárquica da Etrnty;
v. Promover a elaboração de relatórios sobre a situação dos controles internos, a serem apreciados e aprovados; e
vi. Assegurar que o sistema de controles internos seja periodicamente revisado e atualizado de forma a garantir sua efetividade.

Capítulo V – Das Responsabilidades

Em atenção ao disposto no artigo 4º, IV, da Resolução CVM 21, a Sociedade indica o Sr. Arthur Pugliesi Goi como responsável pela implantação de práticas de negócio eficientes e controles internos adequados e eficazes ("Responsável por Controles Internos").

Todo e qualquer gestor que integrar a área será responsável por estabelecer, manter, promover e avaliar as práticas de negócio eficientes e controles internos adequados e eficazes.

As políticas da Etrnty abordam os seguintes aspectos, dentre outros:

i. Conduta e Ética;
ii. Investimentos Pessoais;
iii. Rateio e Divisão de Ordens;
iv. Gestão de Riscos;
v. Segurança de Informações;
vi. Proteção à Lavagem de Dinheiro e Corrupção;
vii. Segregação de Atividades.

O Responsável por Controles Internos será o encarregado pela definição dos métodos para avaliação e monitoramento do sistema de controles internos da Sociedade, sendo também responsável pelo atendimento aos Órgãos Reguladores e Autorreguladores.

A periodicidade e os exames para avaliação do sistema de controles internos a serem realizados serão definidos pelo Responsável por Controles Internos.

O Responsável por Controles Internos será o encarregado por acompanhar o resultado dos testes das avaliações e supervisionar as atividades de controles internos da Sociedade, bem

como por monitorar a qualidade e integridade dos mecanismos de controles internos da Etrnty, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias.

A Sociedade emitirá um relatório anual de controles internos com (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento quando necessário; e (iii) a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco, a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las, que ficará disponível para a CVM na sede da Etrnty, conforme artigo 25, da Resolução CVM 21.

Capítulo VI – Processo de Controles Internos

De forma colaborativa, cada Integrante é responsável pela observância dos controles internos, a fim de mitigar qualquer impacto para seus clientes ou negócios da Sociedade. Assim, com o objetivo de manter altos padrões de integridade e valores éticos e buscando a participação de todos seus colaboradores no processo de controles internos, a Sociedade atua de modo a disseminar, manter e aprimorar a cultura de governança, de modo que tenham conhecimento de forma clara, dos papéis e responsabilidades no sistema e controles internos.

Neste contexto, a Sociedade garante a existência de canais de comunicação que assegurem a todos os Integrantes a comunicação a respeito de eventuais violações referentes ao cumprimento das normas e às informações consideradas relevantes no desempenho de suas atividades, como forma de controle interno, de modo que tais canais de comunicação encontram-se definidos e disponibilizados no *website* da Sociedade.

Paralelamente ao controle preventivo atribuído a cada um dos Integrantes, a Sociedade mantém o controle atribuído à área de *compliance*, consolidada dentro da diretoria de controles internos, para avaliar as atividades desenvolvidas e proceder aos apontamentos, que deverão ser procedidos mediante emissão de relatório elaborado periodicamente, resultantes de controle interno preventivo.

Capítulo VII – Investimentos Pessoais

Todo e qualquer investimento pessoal deverá seguir os termos, regras e condições da Política de Negociação de Valores Mobiliários da Sociedade, disponível no site https://www.etrnty.com.br/.

Capítulo VIII – Sigilo e Conduta

Todos os Integrantes deverão ler atentamente e entender o disposto nesta Política, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no Anexo I ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da Sociedade. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da Sociedade.

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

(i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Sociedade;
(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Sociedade;
(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
(v) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Sociedade e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Sociedade e que ainda não foi devidamente levado à público;
(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
(viii) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da Sociedade ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Integrantes ou a Integrantes não autorizados, não só durante a vigência de seu relacionamento profissional com a Sociedade, mas também após o seu término

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

Sem prejuízo da colaboração da Sociedade com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais e/ou administrativas, deverá ser prévia e tempestivamente informada ao Responsável por Controles Internos, para que este decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Caso os Integrantes tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Responsável por Controles Internos, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Integrantes que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Responsável por Controles Internos.

Capítulo IX – Insider Trading, "Dicas" e Front-running

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem: **(a)** *Insider Trading*, ou seja, a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Integrantes); **(b)** "Dica", ou seja, a transmissão, a qualquer terceiro, estranho às atividades da Sociedade, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários; e/ou **(c)** *Front-running*, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas aqui descritas para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Integrante às penalidades descritas na legislação aplicável, incluindo eventual demissão por justa causa.

Capítulo X – Divulgação de Fatos Relevantes

Em que pese seja responsabilidade do administrador fiduciário do fundo a operacionalização da divulgação de qualquer fato relevante ocorrido ou relacionado ao funcionamento do fundo, da classe ou aos ativos integrantes da carteira, assim que dele tiver conhecimento, é responsabilidade dos demais prestadores de serviços, incluindo a Sociedade, informar imediatamente ao administrador fiduciário sobre os fatos relevantes de que venham a ter conhecimento, para a devida divulgação.

Nesse sentido, são considerados relevantes, nos termos do artigo 64, §1º da Parte Geral da Resolução CVM 175, quaisquer fatos que possam influir de modo ponderável no valor das cotas ou na decisão dos investidores de adquirir, resgatar, alienar ou manter cotas.

A seguinte lista não é exaustiva e apresenta exemplos de fatos potencialmente relevantes:

- alteração no tratamento tributário conferido ao fundo, à classe ou aos cotistas;
- contratação de formador de mercado e o término da prestação desse serviço;
- contratação de agência de classificação de risco, caso não estabelecida no regulamento do fundo ou no anexo da classe;
- mudança na classificação de risco atribuída ao fundo, à classe ou à subclasse de cotas;
- alteração de prestador de serviço essencial;
- fusão, incorporação, cisão ou transformação do fundo ou da classe de cotas;
- alteração do mercado organizado em que seja admitida a negociação de cotas do fundo;
- cancelamento da admissão das cotas do fundo ou da classe à negociação em mercado organizado; e
- emissão de cotas de fundo fechado.

Os fatos relevantes podem, de formar excepcional, deixar de ser divulgados, caso seja entendido pela Sociedade e pelo administrador fiduciário do fundo que sua revelação põe em risco interesse legítimo dos fundos ou de seus cotistas. Neste caso, tais informações serão tratadas como confidenciais até a Sociedade julgar como oportuno o momento para sua divulgação.

Por outro lado, o administrador fiduciário fica obrigado a divulgar imediatamente fato relevante na hipótese de a informação escapar ao controle ou se ocorrer oscilação atípica na cotação, preço ou quantidade negociada de cotas, em havendo negociação em mercado regulado. A Sociedade deverá notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

A Sociedade deverá disponibilizar os fatos relevantes relativos aos fundos sob sua gestão em seu website.

Capítulo XI – Treinamento e Processo de Reciclagem

A Sociedade possui um processo de treinamento **inicial** de todos os seus Integrantes, especialmente aqueles que tenham acesso às Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Assim que cada Integrante for contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Sociedade e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Neste sentido, a Sociedade adota um programa de reciclagem **anual** dos seus Integrantes, à medida que as normas, princípios, conceitos e valores contidos nesta Política sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

Capítulo XII – Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Responsável por Controles Internos e exige o comprometimento total dos Integrantes quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Sociedade, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Política (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Integrantes decorrentes do descumprimento de tais regras.

O Responsável por Controles Internos poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.

Capítulo XIII – Políticas de Segurança da Informação e Segurança Cibernética

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Sociedade e às disposições desta Política, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da Sociedade são protegidas por controles de entrada apropriados para assegurar a segurança dos Integrantes e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho não serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Integrante responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Sociedade.

A execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Equipe de Compliance e Risco que será responsável inclusive por sua revisão, realização de testes e treinamento dos Integrantes, conforme descrito nesta Política.

- Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a Sociedade identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Integrantes e da própria Sociedade, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
(ii) Sistemas: Informações sobre os sistemas utilizados pela Sociedade e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
(iii) Processos e Controles: Processos e controles internos que sejam parte da rotina das áreas de negócio da Sociedade; e
(iv) Governança da Gestão de Risco: Eficácia da gestão de risco pela Sociedade quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Sociedade identificou as

seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

(i) *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
(ii) Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
(iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
(iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Sociedade avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

➢ <u>Ações de Prevenção e Proteção</u>

Após a identificação dos riscos, a Sociedade adota as medidas a seguir descritas para proteger Informações Confidenciais e sistemas.

- Regra Geral de Conduta

A Sociedade realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Integrantes que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Integrantes façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Sociedade e circulem em ambientes externos à Sociedade com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o Integrante que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Integrantes da Sociedade deve sempre se pautar 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 Equipe de Compliance e Risco deve ser acionada previamente à revelação.

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

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

A Sociedade não mantém arquivo físico centralizado, sendo cada Integrante responsável direto pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

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

Em consonância com as normas internas acima, os Integrantes devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Sociedade. É proibida a conexão de equipamentos na rede da Sociedade que não estejam previamente autorizados pelos administradores da Sociedade.

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 difamar a imagem e afetar a reputação da Sociedade.

O recebimento de e-mails muitas vezes não depende do próprio Integrante, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Neste caso, o Integrante deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Sociedade.

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

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema
O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Responsável por Controles Internos e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Integrantes. A Sociedade mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Integrantes. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Sociedade necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Sociedade em caso de violação.
Senha e Login
A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas **semestralmente**, conforme aviso fornecido pelo responsável pela área de informática. Dessa forma, o Integrante pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.
Uso de Equipamentos e Sistemas
Cada Integrante é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. A utilização dos ativos e sistemas da Sociedade, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional. Todo Integrante deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Integrante identifique a má conservação,

uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Responsável por Controles Internos.

Acesso Remoto

A Sociedade permite o acesso remoto pelos Integrantes ao e-mail, rede e diretório, conforme requisição por estes e autorização pelo Responsável por Controles Internos.

Ademais, os Integrantes autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Responsável por Controles Internos qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Sociedade e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

Controle de Acesso

O acesso de pessoas estranhas à Sociedade a áreas restritas somente é permitido com a autorização expressa de Integrantes autorizados pelo Responsável por Controles Internos.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Integrantes, a Sociedade monitora a utilização de tais meios.

Firewall*, *Software*, Varreduras e *Backup

A Sociedade utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Responsável por Controles Internos é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Sociedade mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras constantes a cada acesso a um determinado arquivo, para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Sociedade.

A Sociedade utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Responsável por Controles Internos é responsável por patches regulares nos sistemas da Sociedade.

A Sociedade mantém e testa regularmente medidas de backup consideradas apropriadas pelo Responsável por Controles Internos. As informações da Sociedade são atualmente objeto de backup periódico com o uso de computação na nuvem.

➢ Monitoramento e Testes

A Equipe de Compliance e Risco adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **anual**:

(i) Monitoramento, por amostragem, do acesso dos Integrantes a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e
(ii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Equipe de Compliance e Risco poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

➢ Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Sociedade (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Responsável por Controles Internos prontamente. O Responsável por Controles Internos determinará quais membros da administração da Sociedade e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Responsável por Controles Internos determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Responsável por Controles Internos responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Sociedade de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da Sociedade, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, a Sociedade ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Responsável por Controles Internos, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

- Arquivamento de Informações

Os Integrantes deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do Artigo 18 e com o Artigo 34 da Resolução CVM 21.

Capítulo XIV – Website da Sociedade

O website da Sociedade deverá disponibilizar as Políticas exigidas pela Resolução CVM 21, bem como os seguintes documentos e informações relativos aos fundos sob gestão, conforme exigido pela regulamentação em vigor:

Documento ou Informação[1]	Base Legal

[1] Os seguintes documentos poderão ser, alternativamente, disponibilizados exclusivamente no site do administrador fiduciário, conforme alinhamento entre os Prestadores de Serviços Essenciais: demonstração de desempenho, lâmina, regulamentos, anexos e apêndices, descrição da tributação aplicável ao Fundo ou à Classe.

Regulamento anexos e apêndices atualizados	Art. 47, Parte Geral, Resolução CVM 175
Descrição da tributação aplicável ao Fundo e/ou Classe	Art. 47, Parte Geral, Resolução CVM 175
Política de Voto	Art. 47, Parte Geral, Resolução CVM 175
As informações periódicas e eventuais de cada Fundo e/ou Classe	Art. 61, Parte Geral, Resolução CVM 175
Fatos Relevantes	Art. 64, §2º, Parte Geral, Resolução CVM 175
Convocação da assembleia de cotistas geral do fundo de investimento e especial das classes e subclasses	Art. 72, Parte Geral da Resolução CVM 175
Identificação dos Prestadores de Serviço contratados	Art. 48, inciso I, Resolução CVM 175
Demonstração de desempenho dos fundos de investimento financeiros	Art. 13 do Anexo I (FIFs), Resolução CVM 175
Lâmina dos fundos de investimento financeiros	Art. 13 do Anexo I (FIFs), Resolução CVM 175

Capítulo XV – Políticas de Certificação

- Introdução

A Etrnty observa as disposições das Regras e Procedimentos de Certificação Anbima, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

- Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Etrnty como gestora de recursos de terceiros, foi identificado que a CGA é a única certificação pertinente às suas atividades, sendo a CGA aplicável aos profissionais da Etrnty com alçada/poder discricionário de investimento.

Nesse sentido, somente o Integrante com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão (conforme definido no Formulário de Referência da Etrnty), ou seja, o Integrante que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA, uma vez que esta certificação é aplicável aos profissionais que atuam em carteiras administradas e/ou fundos de investimento financeiro.

Em complemento, a Etrnty destaca que as certificações são de cunho pessoal e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Responsável por Controles Internos, sendo certo que caso o Integrante esteja exercendo a atividade elegível de CGA na Etrnty e a certificação não esteja vencida, a partir do vínculo do Integrante com a Etrnty, o prazo de validade da certificação CGA será indeterminado, enquanto perdurar o seu vínculo com a Etrnty e a sua atuação na atividade elegível. Por outro lado, caso o Integrante não esteja exercendo a atividade elegível da CGA na Etrnty, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível da CGA.

- Identificação de Profissionais Certificados e Atualização do Banco de Dados

Antes da contratação, admissão ou transferência de área de qualquer Integrante, a Equipe de Compliance e Risco deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Integrante o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Integrante possui alguma certificação ANBIMA, uma vez que, em caso positivo, a Etrnty deverá inserir o Integrante no Banco de Dados.

O Diretor de Gestão deverá esclarecer à Equipe de Compliance e Risco se os Integrantes que integrarão o departamento técnico envolvido na gestão de recursos terão ou não alçada/poder discricionário de decisão de investimento e com quais produtos cada um dos Integrantes irá atuar.

Caso seja identificada a necessidade de certificação, a Equipe de Compliance e Risco deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Integrante.

A Equipe de Compliance e Risco também deverá checar se os Integrantes que estejam se desligando da Etrnty estão indicados no Banco de Dados como profissionais elegíveis/certificados vinculados à Etrnty, sendo, para estes, obrigatória a inclusão do desligamento no Banco de Dados.

A Equipe de Compliance e Risco deve incluir no Banco de Dados as informações cadastrais de todos os Integrantes que tenham qualquer certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização, sendo referida inclusão facultativa somente para estagiários e terceiros contratados.

Todas as atualizações no Banco de Dados devem ocorrer **até o último dia útil do mês subsequente à data do evento que deu causa a atualização**, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela Equipe de Compliance e Risco, conforme disposto abaixo.

- Rotinas de Verificação

Semestralmente, a Equipe de Compliance e Risco deverá verificar as informações contidas no Banco de Dados, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos nas Regras e Procedimentos de Certificação Anbima.

Ainda, o Diretor de Gestão deverá contatar a Equipe de Compliance e Risco **prontamente**, sempre que houver algum tipo de alteração nos cargos/funções dos Integrantes que integram o departamento técnico envolvido na gestão de recursos e/ou com quais produtos cada destes Integrantes atuarem, confirmando, além disso, todos aqueles Integrantes que atuem com alçada/poder discricionário de investimento, se for o caso.

Integrantes que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação) estão impedidos de ordenar a compra e venda de ativos sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela Equipe de Compliance e Risco, caso seja verificada qualquer irregularidade com as funções exercidas por um Integrante, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Gestão por profissionais não certificados ou, de maneira geral, que o Integrante está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, o Responsável por Controles Internos deverá declarar, de imediato, o afastamento do Integrante, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Integrante, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, **anualmente**, deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento das Regras e Procedimentos de Certificação Anbima, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

- Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais haja certificação exigível, nos termos previstos desta Política, serão imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem ou até que o Conselho de Certificação conceda a isenção de obtenção da certificação aplicável, devendo para tanto assinar a documentação prevista no **Anexo II** a este Manual, comprovando o seu afastamento da Etrnty.

Capítulo XII – Da Vigência e Atualização

Esta Política de Controles Internos será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência. Qualquer alteração à presente Política será amplamente divulgada a todos os Integrantes da Etrnty pelo Responsável por Controles Internos.

***

ANEXO I
TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____, doravante denominado Integrante, e Etrnty Capital Gestora de Recursos Ltda. ("Etrnty" ou "Sociedade").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Sociedade, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Sociedade, seus sócios e clientes, aqui também contemplados os próprios fundos, incluindo:

a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Sociedade;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Sociedade;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Sociedade ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Sociedade e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Sociedade ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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

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

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Integrante entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Integrante obrigado a indenizar a Sociedade, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Integrante tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Integrante reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Sociedade são e permanecerão sendo propriedade exclusiva da Sociedade e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Sociedade, devendo todos os documentos permanecer em poder e

sob a custódia da Sociedade, salvo se em virtude de interesses da Sociedade for necessário que o Integrante mantenha guarda de tais documentos ou de suas cópias fora das instalações da Sociedade;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Integrante, o Integrante deverá restituir imediatamente à Sociedade todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Sociedade, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Integrante ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Integrante deverá notificar imediatamente a Sociedade, permitindo que a Sociedade procure a medida judicial cabível para atender ou evitar a revelação.

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

5.2. A obrigação de notificar a Sociedade subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Integrante, por prazo indeterminado.

6. Tenho ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD") e me comprometo a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas em conformidade com o estabelecido

pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Sociedade.

6.1. Estou ciente, ainda, de meu compromisso de comunicar ao Encarregado[2], conforme definido pela Sociedade, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Sociedade.

6.2. Na qualidade de pessoa física titular de Dados Pessoais ("Titular de Dados Pessoais"), estou ciente e de acordo que a Sociedade, na qualidade de "Controladora" para fins de atendimento às disposições da LGPD, tome decisões relativas ao Tratamento de meus Dados Pessoais[3], incluindo operações 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 ("Tratamento") durante todo o período em que eles forem pertinentes, observados os princípios e as garantias ora estabelecidas pela referida lei.

6.3. Também na qualidade de Titular de Dados Pessoais, estou ciente de que, a qualquer tempo, mediante requisição à Controladora, tenho o direito de (i) confirmar a existência de Tratamento e acessar meus Dados Pessoais, (ii) corrigir dados incompletos, inexatos ou desatualizados, (iii) solicitar a anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD, (iv) solicitar a portabilidade de meus Dados Pessoais a outro fornecedor de serviço, (v) solicitar a eliminação dos Dados Pessoais tratados com o meu consentimento, (vi) solicitar informações sobre o compartilhamento dos meus dados pela Controladora e sobre a possibilidade de não fornecer o consentimento e as consequências dessa negativa, e (vii) me opor ao Tratamento de meus Dados Pessoais em caso de descumprimento da LGPD.

6.4. Reconheço que a Controladora poderá compartilhar os Dados Pessoais com outros agentes de Tratamento de dados, tais como escritórios de contabilidade, agências de turismo, planos de saúde e instituições financeiras, caso seja necessário, bem como que poderá compartilhar em seu website os Dados Pessoais, incluindo minha identificação como Integrante da Sociedade e meu histórico profissional, observados os princípios e as garantias ora estabelecidas pela LGPD, com o que, desde já, estou de acordo.

---

[2] "Encarregado" é a pessoa indicada pela Sociedade para atuar como canal de comunicação entre os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados.

[3] Para os fins do presente Termo de Compromisso são considerados Dados Pessoais toda informação relacionada a uma pessoa física que a torne diretamente identificada ou identificável.

6.5. Estou ciente de que a Controladora poderá manter armazenados os Dados Pessoais necessários após o término da relação contratual, por prazo determinado em lei, para fins de cumprimento de obrigações legais e/ou regulatórias, bem como para exercer seus direitos em processos administrativos e/ou judiciais.

6.6. Comprometo-me, enfim, a observar em tudo às instruções fornecidas pela Sociedade, na qualidade de Controladora, acerca do Tratamento que deverá ser concedido aos Dados Pessoais aos quais tiver acesso em razão de minhas atividades, bem como a sempre agir de acordo com as disposições da LGPD e das normas internas da Sociedade quanto à privacidade e proteção de Dados Pessoais.

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

8. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Integrante às sanções que lhe forem atribuídas pelos sócios da Sociedade.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Cidade], [---] de [---] de [---].

_____

[INTEGRANTE]

_____

Etrnty Capital Gestora de Recursos Ltda.

Testemunhas:

1._____
Nome:
CPF/MF:

2._____
Nome:
CPF/MF:

ANEXO II
TERMO DE AFASTAMENTO

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de alçada/poder final de decisão de investimentos e/ou desinvestimentos dos fundos sob gestão da Etrnty Capital Gestora de Recursos Ltda. ("Etrnty" ou "Sociedade") por prazo indeterminado:

[ ] até que me certifique pela CGA; ou

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGA.

[Cidade], [---] de [---] de [---].

_____
[INTEGRANTE]

_____
Etrnty Capital Gestora de Recursos Ltda.

Testemunhas:

1._____
Nome:
CPF/MF:

2._____
Nome:
CPF/MF: