



# Manual de Regras, Procedimentos e Descrição dos Controles Internos do Grupo Stratus

*(Revisão: Junho de 2022)*



1.	INTRODUÇÃO .....	4
1.1.	Grupo Stratus .....	4
1.2.	Atividades do Grupo Stratus .....	4
1.3.	O Manual .....	4
1.4.	Responsabilidades e Obrigações .....	4
1.5.	Conhecimento e Aplicação do Manual .....	4
1.6.	Revisão periódica do Manual .....	5
2.	ÁREA DE COMPLIANCE .....	5
2.1.	Diretor de Compliance .....	5
2.2.	Requisitos para a nomeação do Diretor de Compliance .....	7
2.3.	Garantia de independência .....	7
2.4.	Exames periódicos .....	7
2.5.	Relatório de Compliance .....	8
2.6.	Dever de informar .....	8
2.7.	Sanções .....	8
3.	POLÍTICA DE CONFIDENCIALIDADE .....	9
3.1.	Confidencialidade .....	9
3.2.	Informações Confidenciais .....	9
3.3.	Compromisso de Confidencialidade .....	10
3.4.	Revelações permitidas .....	10
3.5.	Limitações .....	10
3.6.	Insider Trading, Dicas e Front-Running .....	11
4.	POLÍTICAS DE SEGURANÇA E SEGURANÇA CIBERNÉTICA .....	12
4.1.	Segurança .....	12
4.2.	Identificação dos Riscos .....	12
4.3.	Ações de Prevenção e Proteção .....	13
4.4.	Armazenamento e Arquivamento de Informações .....	16
4.5.	Monitoramento e Testes .....	17
4.6.	Plano de Identificação e Resposta .....	17
4.7.	Treinamento .....	18
4.8.	Revisão da Política .....	18
5.	PROGRAMA DE TREINAMENTO .....	18
5.1.	Treinamentos periódicos .....	18

5.2.	Participação nos treinamentos .....	18
5.3.	Condições dos treinamentos.....	19
6.	SEGREGAÇÃO DE ATIVIDADES.....	19
6.1.	Segregação de atividades de administração de carteiras de valores mobiliários:.....	19
7.	REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS DO GRUPO STRATUS .....	20
7.1.	Regras, procedimentos e controles internos .....	20
8.	CONTROLE DE VERSÕES .....	22
ANEXO 1.5 – TERMO DE ADESÃO AO CÓDIGO.....		23
ANEXO 3.3 – Modelo de Compromisso de Confidencialidade.....		24

## 1. INTRODUÇÃO

### 1.1. Grupo Stratus

A Stratus Capital S.A. em conjunto com as empresas que sejam ou venham ser suas controladoras, controladas, coligadas ou sob controle comum, são referidas neste documento como “Grupo Stratus”, incluindo a Stratus Investimentos Ltda. (“Administradora”) e a Stratus Gestão de Carteiras Ltda. (“Gestora”). Administradora e Gestora são empresas autorizadas pela Comissão de Valores Mobiliários (“CVM”) a desenvolver o exercício profissional de atividades relacionadas à administração de carteiras de valores mobiliários nos termos da Resolução CVM nº 21 de 25 de fevereiro de 2021 (“Res. CVM 21”).

### 1.2. Atividades do Grupo Stratus

As principais atividades desenvolvidas pelo Grupo Stratus são relacionadas à execução de carteiras e fundos de investimento em modelo funcional e fiduciário internacionalmente caracterizado como *General Partner* (“GP”). Administradora e Gestora exercem no Brasil atividades de administração de carteira de valores mobiliários (respectivamente, administração fiduciária e gestão discricionária) em relação aos veículos de investimento (“Fundos”). A Administradora também atua na distribuição de cotas de Fundos sob sua administração, nos termos do Art. 33 da Res. CVM 21.

### 1.3. O Manual

O Grupo Stratus adota o presente **Manual de Regras, Procedimentos e Descrição dos Controles Internos** (“Manual”) detalhando procedimentos e controles relacionados às suas atividades. e tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança (“Colaboradores”) no, ou com o Grupo Stratus, tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Este Manual foi elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/nº 05/2014, com a Res. CVM 21, e demais normas e orientações da CVM e da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (“ANBIMA”), incluindo o Manual ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros (“Manual ANBIMA de ART”), Manual ANBIMA de Ética (“Manual ANBIMA de Ética”) e Manual ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada (“Manual ANBIMA de Certificação”).

### 1.4. Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do Diretor de Compliance, conforme definido no item 2.1. abaixo.

### 1.5. Conhecimento e Aplicação do Manual

O Manual, assim como as demais normas e políticas do Grupo Stratus, é apresentado a todos os Colaboradores, que devem assinar o Termo de Adesão ao Manual (Anexo 1.5 ao Manual),

confirmando seu compromisso de observar e aplicar o Manual. Essa apresentação é feita por ocasião do ingresso do Colaborador e reiterada com periodicidade no mínimo anual.

### **1.6. Revisão periódica do Manual**

O Manual deverá ser revisado periodicamente, pelo menos a cada dois anos, pelo Diretor de Compliance, conforme definido no item 2.1. abaixo, ou sempre que forem identificadas mudanças relevantes na legislação ou regulamentação aplicável aos investimentos em *private equity* relacionados aos temas abordados.

## **2. ÁREA DE COMPLIANCE**

### **2.1. Diretor de Compliance**

Os sócios da Administradora e da Gestora devem nomear, nos respectivos Contratos Sociais, uma mesma pessoa como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos previstos neste Manual e na Res. CVM 21 (“Diretor de Compliance”).

São obrigações do Diretor de Compliance:

- i. Acompanhar as políticas descritas neste Manual;
- ii. Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade do Grupo Stratus para apreciação dos administradores do Grupo Stratus;
- iii. Atender prontamente todos os Colaboradores;
- iv. Identificar possíveis condutas contrárias a este Manual e todas as demais políticas e manuais do Grupo Stratus;
- v. Centralizar informações e revisões periódicas dos processos de compliance, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;
- vi. Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;
- vii. Encaminhar aos órgãos de administração do Grupo Stratus, até o último dia útil do mês de abril de cada ano, relatório referente ao ano civil imediatamente anterior à data de entrega, contendo:
  - a) as conclusões dos exames efetuados;
  - b) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
  - c) 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; devendo referido relatório permanecer disponível à CVM na sede do Grupo Stratus;
- d) relatório anual listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Combate e Prevenção à Lavagem de Dinheiro, do Grupo Stratus, nos termos da Resolução CVM nº 50.
- viii. Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- ix. Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;
- x. Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;
- xi. Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- xii. Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria externa ou outros assessores profissionais;
- xiii. Aplicar as eventuais sanções aos Colaboradores; e
- xiv. Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:
- a) Investimentos pessoais;
  - b) Transações financeiras com clientes fora do âmbito do Grupo Stratus;
  - c) Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
  - d) Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
  - e) Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
  - f) Participações em alguma atividade política.

O Diretor de Compliance poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de compliance e de risco, com as atribuições a serem definidas caso a caso, a depender

da necessidade da Administradora e da Gestora em razão de seu crescimento e de acordo com a senioridade do Colaborador.

## **2.2. Requisitos para a nomeação do Diretor de Compliance**

A pessoa nomeada como Diretor de Compliance poderá exercer outras funções no Grupo Stratus ou fora dele, sendo vedada a atuação em funções relacionadas à administração de recursos de terceiros, à intermediação, distribuição ou à consultoria de valores mobiliários, ou em qualquer atividade que limite a sua independência.

## **2.3. Garantia de independência**

Os Colaboradores que desempenharem as atividades de compliance formarão a Área de Compliance, sob a coordenação do Diretor de Compliance, sendo certo que a Área de Compliance exerce suas atividades de forma completamente independente das outras áreas do Grupo Stratus e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

## **2.4. Exames periódicos**

O Diretor de Compliance será responsável por fazer exames periódicos durante o ano a fim de identificar se a(s) empresa(s) do Grupo Stratus na(s) qual(is) esteja ocupando tal função está(ão) em plena conformidade com a Res. CVM 21, com este Manual e com outras normas aplicáveis à atividade.

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades do Grupo Stratus, que cheguem ao conhecimento do Diretor de Compliance, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelo Diretor de Compliance, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pelo Grupo Stratus.

Adicionalmente, será realizado um monitoramento anual, a cargo do Diretor de Compliance, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

O Diretor de Compliance poderá utilizar as informações obtidas em tais sistemas para decidir acerca de eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu

conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

Adicionalmente, o Diretor de Compliance deverá ainda verificar, anualmente, os níveis de controles internos e compliance junto a todas as áreas do Grupo Stratus, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas do Grupo Stratus, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, o Diretor de Compliance poderá, quando julgar oportuno e necessário, realizar inspeções nas ferramentas de trabalho de quaisquer Colaboradores a qualquer momento.

Por fim, ao menos uma vez a cada dois anos, a Área de Compliance deverá conduzir uma revisão completa de todo Programa de Compliance – que inclui este Manual, a agenda regulatória, o programa de treinamento (inclusive da própria Área de Compliance), formulários e testes de aderência.

## **2.5. Relatório de Compliance**

A Área de Compliance, sob condução e responsabilidade final do Diretor de Compliance, é responsável pela emissão do relatório descrito no Artigo 25 da Res. CVM 21<sup>1</sup> (“Relatório”), observando os prazos e conteúdo mínimo descritos na norma. Os demais Colaboradores deverão apresentar informações e documentos solicitados pelo Diretor de Compliance para a elaboração do Relatório dentro do prazo indicado por este. O Diretor de Compliance deve: (i) enviar cópias (físicas e/ou digitalizadas) do Relatório aos Diretores Executivos da(s) empresa(s) do Grupo Stratus na(s) qual(is) esteja ocupando tal função e (ii) manter na sede da empresa uma via (física ou digitalizada) do Relatório disponível para a CVM.

## **2.6. Dever de informar**

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento ao Diretor de Compliance.

Todos os comunicados e investigações serão tratados de maneira confidencial, na medida do possível.

Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. Contudo, o Colaborador que se omitir de tal obrigação poderá sofrer além de ação disciplinar, demissão por justa causa, conforme regime jurídico.

## **2.7. Sanções**

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade do Diretor de Compliance, garantido ao Colaborador amplo direito de defesa.

Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios do Grupo Stratus, ou demissão por justa causa, no caso de Colaboradores que sejam empregados do Grupo Stratus, nesse último caso, nos termos do artigo 482 da Consolidação das Leis do Trabalho (“CLT”), sem prejuízos do direito do Grupo Stratus de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

O Grupo Stratus não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso o Grupo Stratus venha a ser responsabilizado ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, pode exercer o direito de regresso em face dos responsáveis.

### **3. POLÍTICA DE CONFIDENCIALIDADE**

#### **3.1. Confidencialidade**

No contexto de suas atividades, o Grupo Stratus tem de lidar com Informações Confidenciais (como definido a seguir, no item 3.2) de clientes e potenciais clientes de todas as suas atividades, empresas investidas, potenciais empresas investidas, etc. Para tanto, empresas do Grupo Stratus entram em acordos de confidencialidades que preveem penalidades no caso de quebra de tal confidencialidade. Esta confidencialidade por vezes inclui o próprio fato de que estejam ocorrendo conversações e negociações, além das próprias informações confidenciais. Com o objetivo de resguardar a privacidade de informações pessoais ou financeiras dos investidores, clientes e empresas investidas, prevalecerá, em regra e em qualquer situação de dúvida, o caráter sigiloso de dados, informações, comunicações, saldos, posições e qualquer outro tipo de informações relativas a clientes do Grupo Stratus e aos fundos geridos e/ou administrados pelo Administrador ou Gestor que não sejam sabidamente de conhecimento público.

#### **3.2. Informações Confidenciais**

São consideradas informações confidenciais, reservadas ou privilegiadas (“Informações Confidenciais”), para os fins deste Manual, 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 o Grupo Stratus, seus sócios e clientes, aqui também contemplados os próprios fundos de investimento sob gestão e/ou administração do Grupo Stratus, 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 de investimento geridos ou administrados pelo Grupo Stratus;

- iii. Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridas ou administradas pelo Grupo Stratus;
- 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 do Grupo Stratus 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 do Grupo Stratus 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 Colaboradores do Grupo Stratus ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral que ainda não tenham sido divulgadas publicamente.

### **3.3. Compromisso de Confidencialidade**

Todos os Colaboradores devem assinar um “Compromisso de Confidencialidade”, na forma do modelo que integra o presente Manual como Anexo 3.3, quando de seu ingresso no Grupo Stratus, que inclui políticas de utilização e autorização de monitoramento dos recursos de informática, internet e telefonia. O não cumprimento do respectivo Compromisso de Confidencialidade estará sujeito à apuração de responsabilidades nas esferas cível e criminal.

### **3.4. Revelações permitidas**

Caso algum Colaborador ou empresa do Grupo Stratus seja compelido a revelar Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, tal Colaborador ou, no caso de empresa, o Colaborador a quem tiver sido dirigida a requisição de revelação, deverá prévia e tempestivamente comunicar o Diretor de Compliance para que este decida sobre a forma mais adequada para tal revelação.

### **3.5. Limitações**

Os Colaboradores não poderão sem a prévia autorização por escrito da empresa do Grupo Stratus a que pertencerem:

- i. levar para fora do local em que trabalhe material interno, inclusive informações financeiras sobre operações de clientes do Grupo Stratus;
- ii. extrair cópia de documentos formalizados em papel e arquivos registrados em meio magnético, que contenham informações do Grupo Stratus, inclusive relativas a clientes e empresas das carteiras de fundos geridos ou administrados por empresas do Grupo Stratus (incluindo potenciais clientes e potenciais empresas investidas);

- iii. transmitir ou transferir para terceiros, por qualquer meio, físico ou eletrônico, informações confidenciais relacionadas às atividades das áreas envolvidas na administração de carteiras e gestão de recursos de terceiros; e
- iv. permitir o acesso de terceiros a sistemas de informações ou operações e bancos de dados de responsabilidade e/ou propriedade do Grupo Stratus.

### **3.6. Insider Trading, Dicas e Front-Running**

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading*, *Dicas* ou *Front-running*, conforme definições a seguir:

- i. *Insider Trading*: significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).
- ii. *Dicas*: é a transmissão, a qualquer terceiro, estranho às atividades do Grupo Stratus, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.
- iii. *Front-running*: significa a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com o Grupo Stratus, mas também após o seu término.

Os Colaboradores 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.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, 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 Colaboradores 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 Diretor de Compliance anteriormente mencionada.

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

#### **4. POLÍTICAS DE SEGURANÇA E SEGURANÇA CIBERNÉTICA**

##### **4.1. Segurança**

As informações confidenciais relativas aos fundos de investimentos geridos e/ou administrados pelo Grupo Stratus, seus investidores existentes e potenciais e empresas investidas ou potencialmente investidas são protegidas por meio do armazenamento seguro e da adoção das melhores práticas de segurança utilizadas no mercado.

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

Todos os equipamentos da rede deverão estar acomodados em salas fechadas, de acesso restrito. As estações de trabalho são fixas, com computadores seguros e as sessões abertas devem ser trancadas quando deixadas sem supervisão do Colaborador 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 pelo Grupo Stratus.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Diretor de Compliance, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

##### **4.2. Identificação dos Riscos**

No âmbito de suas atividades, o Grupo Stratus identificou os seguintes principais riscos internos e externos que precisam de proteção:

- i. **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e do próprio Grupo Stratus, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão ou administração, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- ii. **Sistemas:** informações sobre os sistemas utilizados pelo Grupo Stratus 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 do Grupo Stratus; e
- iv. **Governança da Gestão de Risco:** a eficácia da gestão de risco pelo Grupo Stratus quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, o Grupo Stratus 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;
- 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 disposto acima, o Grupo Stratus 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.

#### **4.3. Ações de Prevenção e Proteção**

Após a identificação dos riscos, o Grupo Stratus adota as medidas a seguir descritas para proteger suas informações e sistemas.

##### **I. Regra Geral de Conduta:**

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

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede do Grupo Stratus e circulem em ambientes externos ao Grupo Stratus 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 do Grupo Stratus. Nestes casos, o Colaborador 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 Colaboradores 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 Área de Compliance deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico do Grupo Stratus 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 do Grupo Stratus.

Cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo ou garantir a entrega de tal documento à área, equipe ou pessoa responsável por seu armazenamento.

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 Colaboradores 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 no Grupo Stratus. É proibida a conexão de equipamentos na rede do Grupo Stratus que não estejam previamente autorizados pela área de tecnologia da informação ou pelo superior imediato do Colaborador.

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 prejudicar a imagem e/ou afetar a reputação do Grupo Stratus.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores do Grupo Stratus.

A visualização de sites, blogs, 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.

## **II. Acesso Escalonado do Sistema**

O acesso como “administrador” de área de desktop é limitado aos usuários aprovados pelo Diretor de Compliance e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

O Grupo Stratus mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede do Grupo Stratus necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas do Grupo Stratus em caso de violação.

## **III. 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 tecnologia da informação), ou combinada com ferramentas de autenticação em dois fatores ("two-factor authentication").

O Colaborador poderá ser responsabilizado caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

## **IV. Uso de Equipamentos e Sistemas**

Cada Colaborador 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 do Grupo Stratus, 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 Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistema deve comunicar a área de tecnologia da informação, que poderá levar a matéria ao Diretor de Compliance, se necessário.

## **V. Acesso Remoto**

O Grupo Stratus permite o acesso remoto pelos Colaboradores, a todos as funcionalidades necessárias ao regular exercício de sua função.

Ademais, os Colaboradores 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 Diretor de Compliance qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações do Grupo Stratus e que ocorram durante o trabalho remoto; e
- iv. não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

## **VI. Controle de Acesso**

O acesso de pessoas estranhas ao Grupo Stratus a áreas restritas somente é permitido com a autorização expressa do Diretor de Compliance.

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 Colaboradores, o Grupo Stratus monitora a utilização de tais meios.

## **VII. Firewall, Software, Varreduras e Backup**

O Grupo Stratus utiliza um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance é responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

O Grupo Stratus 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 das empresas (por exemplo, vírus, worms, spyware). Serão conduzidas varreduras semestrais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede do Grupo Stratus.

O Grupo Stratus utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance é responsável por patches regulares nos sistemas do Grupo Stratus.

### **4.4. Armazenamento e Arquivamento de Informações**

As informações confidenciais são mantidas em bases de dados e aplicações em “cloud”, utilizando serviços terceirizados de boa reputação, com links de internet redundantes, e softwares de monitoramento. São realizadas cópias de segurança dos documentos contendo informações confidenciais (backup) diariamente.

Adicionalmente, de acordo com o disposto neste Manual, os Colaboradores 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, em conformidade com o inciso IV do Artigo 18 da Resolução CVM nº 21.

#### **4.5. Monitoramento e Testes**

O Diretor de Compliance (ou pessoa por ele incumbida) 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, semestral:

- i. Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, 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.

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

#### **4.6. Plano de Identificação e Resposta**

##### **I. Identificação de Suspeitas**

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos do Grupo Stratus (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 Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração do Grupo Stratus e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

##### **II. Procedimentos de Resposta**

O Diretor de Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos do Grupo Stratus 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 e/ou administração do Grupo Stratus, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
- vii. Determinação do responsável que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

#### **4.7. Treinamento**

O Diretor de Compliance organizará treinamento anual dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme descrito no item 5 abaixo).

#### **4.8. Revisão da Política**

O Diretor de Compliance realizará uma revisão desta Política de Segurança e Segurança Cibernética a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais do Grupo Stratus e acontecimentos regulatórios relevantes.

### **5. PROGRAMA DE TREINAMENTO**

#### **5.1. Treinamentos periódicos**

Os Colaboradores que tenham acesso a informações confidenciais, que participem do processo de decisão de investimento ou que participem de processos relacionados à distribuição de cotas de fundos de investimento devem participar de treinamentos periódicos. Os treinamentos abrangem as políticas e procedimentos adotados pelo Grupo Stratus e são compatíveis com a atividade desempenhada pelo Colaborador.

#### **5.2. Participação nos treinamentos**

A adesão de cada Colaborador a este Manual implica a obrigação de submeter-se, durante o período que permanecer no Grupo Stratus, ao programa de treinamento ministrado pelas empresas do Grupo Stratus ou por empresas contratadas para esta finalidade, o qual abrangerá, pelo menos:

- i. Discussão sobre os termos e condições deste Manual e consequências decorrentes da não observância do mesmo;

- ii. Normas de confidencialidade quanto às informações dos investidores e demais clientes dos fundos de investimentos administrados e/ou geridos pelas empresas do Grupo Stratus, bem como das empresas investias ou potencialmente investidas;
- iii. Regras quanto à comunicação (artigos, entrevistas ou conversas ainda que informais com empresas de mídia);
- iv. Situações que configurem conflitos de interesse e procedimentos a serem tomados;
- v. Regras relativas à aquisição de ativos negociados no mercado pelos Colaboradores do Grupo Stratus;
- vi. Certificações a serem obtidas e cursos a serem frequentados pelos Colaboradores enquanto vinculados ao Grupo Stratus; e
- vii. Princípios que regem as atividades do Grupo Stratus.

### **5.3. Condições dos treinamentos**

Os treinamentos e atualizações serão ministrados nos horários e dias agendados pelo Grupo Stratus. Eventuais conflitos de agenda deverão ser comunicados ao Diretor de Compliance para que se possa agendar outra data para o treinamento ou atualização.

Os Colaboradores deverão frequentar os cursos externos que o Grupo Stratus determinar. Os custos de tais cursos serão arcados pelo Grupo Stratus e eventual não conclusão ou ausência injustificada de um Colaborador o obrigará a ressarcir o Grupo Stratus.

## **6. SEGREGAÇÃO DE ATIVIDADES**

### **6.1. Segregação de atividades de administração de carteiras de valores mobiliários:**

O Grupo Stratus pratica a segregação de atividades de administração fiduciária e de gestão de carteiras, mantendo equipes diferentes que respondem a diretores diferentes e independentes entre si (nomeados nos termos da Res. CVM 21 nos respectivos contratos sociais da Administradora e a Gestora). O acesso aos arquivos físicos e digitais são restritos aos componentes da própria equipe.

O Grupo Stratus adota as seguintes formas de segregação de negócios e/ou de processos:

#### **A. Segregação de atividades e funções**

O Grupo Stratus segue um sistema de segregação de atividades baseado nas diferenças funcionais de atuação. Perfis de acesso físico e eletrônico, e o controle dos respectivos acessos são realizados com base nessas divisões. Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade (“as-needed basis”), sendo que os Colaboradores se responsabilizam pelo sigilo de quaisquer informações não públicas a que tenham acesso em função de seu cargo.

**B. Segregação física**

A segregação física é feita através do uso de controles de acesso entre as áreas de trabalho da Administradora, uma vez que ela está alocadas no mesmo imóvel que a Gestora. A liberação de acesso e o monitoramento destes são autorizados pelo Diretor de Compliance que avalia quais as áreas cada sócio ou Colaborador necessita ter acesso para o exercício de suas atividades.

Áreas confidenciais e/ou com conflito de interesses são separadas por empresa e espaço, existindo portas com controles de acesso entre as áreas, de forma a cumprir com as obrigações regulatórias que lhes são exigíveis.

**C. Segregação Eletrônica**

O Grupo Stratus implementou uma estrutura de rede que permite restrição de acesso à informação entre áreas confidenciais e/ou com conflito de interesses. A segregação virtual, que envolve a rede, sistemas e dados, é feita através do uso de controles de acesso entre as áreas de trabalho. A liberação de acesso e o monitoramento destes são realizados pelo Diretor de Compliance que avalia quais as áreas cada Colaborador necessita ter acesso para o exercício de suas atividades. Há restrição de acesso a sistemas entre áreas confidenciais e/ou com conflito de interesses, como por exemplo, uso de redes com sistemas segregados para os computadores das áreas.

**7. REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS DO GRUPO STRATUS****7.1. Regras, procedimentos e controles internos**

As regras, procedimentos e controles internos do Grupo Stratus, elaborados para o cumprimento da Res. CVM 21 têm por objetivo a verificação da conformidade das atividades de administração fiduciária e gestão discricionária de ativos com as leis vigentes no País, bem como as políticas do Grupo Stratus e os regulamentos dos fundos de investimentos administrados ou geridos pelo Grupo Stratus.

Os procedimentos de controles internos adotados pelo Grupo Stratus compreendem os seguintes temas: Transações; Confidencialidade; Arquivamento de Documentação de Atos Praticados pelos Fundos e Carteiras Administradas ou Geridas pelo Grupo Stratus; Verificação de Padrões Éticos Aplicáveis à Atividade de Gestão Discricionária de Ativos; e Verificação de Critérios Utilizados para Aferição e Auditoria de Ativos Geridos pela Gestora.

**I. Transações**

No intuito de proteger os interesses dos investidores, o Grupo Stratus efetiva as seguintes verificações durante o processo de realização de transações de investimento ou desinvestimento em empresas das carteiras que compõem os fundos geridos ou administrados pelo Grupo Stratus:

- i. Verificação de toda documentação que reflita a transação (tais como contratos de subscrição, compra e venda, acordos de acionistas, etc.), de modo a identificar possíveis irregularidades, fraudes ou informações inverídicas. Esta etapa também compreende a análise da documentação buscando atender aos objetivos de

- investimento dos cotistas previstos nos regulamentos atinentes aos fundos geridos ou administrados pelo Grupo Stratus;
- ii. Recebimento do ativo após aprovação da transação pelos órgãos internos do respectivo fundo, bem como após efetivação do pagamento que deverá ser sucedido pela consecução dos passos formais pertinentes à transação que objetivem formalizar o supracitado recebimento do ativo (incluindo verificação dos livros societários ou registros escriturais pertinentes, conforme o caso); e
  - iii. Liquidação financeira mediante recebimento do comprovante da operação bancária relativa à transação, que por sua vez deverá ser sucedida pela devida consumação dos passos formais inerentes à conclusão da transação.

Todas as transações relacionadas aos fundos e clientes (por exemplo, pagamentos de despesas ou encargos dos fundos) são devidamente documentadas por um Colaborador e verificadas por outro, de forma a reduzir potenciais erros. Os documentos são armazenados conforme descrito a seguir.

## **II. Arquivamento de Documentação de Atos Praticados pelos Fundos e Carteiras Administradas ou Geridas pelo Grupo Stratus**

Tendo em vista o cumprimento de leis e normas vigentes no País, o Grupo Stratus armazena, durante o período aplicável a cada caso, todos os documentos referentes às suas atividades e aos atos praticados em função destas, em sua sede, em armários devidamente munidos de fechaduras cujas chaves são de responsabilidade dos Colaboradores incumbidos das respectivas atividades. Ademais, o Grupo Stratus verifica, periodicamente, e em duplo grau de checagem, se todos os documentos estão armazenados em conformidade com os padrões temporalmente e espacialmente exigíveis na forma da lei.

## **III. Confidencialidade**

Os procedimentos de verificação do cumprimento dos mandamentos éticos, contratuais e legais de confidencialidade do Grupo Stratus compreendem:

- i. Verificação aleatória das caixas de e-mail de seus Colaboradores em comunicações exteriores, de modo a garantir a observância e o controle dos atos de seus Colaboradores, de sorte que se garanta a conformidade destes atos com as políticas do Grupo Stratus;
- ii. Assinatura de contratos de confidencialidade com possíveis empresas investidas, prestadores de serviço e equiparados, buscando resguardar contratualmente as informações privilegiadas e de interesse de cotistas e clientes; e
- iii. Arquivamento de contratos de confidencialidade, bem como controle dos mesmos, com manutenção de planilha atualizada dos contratos vencidos, vincendos, bem como daqueles sujeitos a prazos adicionais condicionados.

## **IV. Verificação de Padrões Éticos Aplicáveis à Atividade de Gestão Discricionária de Ativos**

Os procedimentos de verificação de padrões éticos aplicáveis à atividade de gestão discricionária de ativos refere-se, sem prejuízo das demais disposições deste Manual e das

políticas do Grupo Stratus, à rigorosa verificação da observância de padrões éticos por parte de todos os envolvidos na gestão de carteiras e recursos de terceiros.

Tal verificação compreende os seguintes procedimentos:

- i. Orientação permanente dos envolvidos na gestão de ativos para que ajam em conformidade com este Manual e as políticas do Grupo Stratus, dentro do programa de treinamentos descrito no capítulo próprio deste Manual; e
- ii. Acompanhamento pelo Diretor de Compliance das reuniões semanais das equipes dedicadas à administração fiduciária e à gestão discricionária de ativos, com foco na identificação de possíveis inconformidades que exijam readequação.

#### **V. Verificação de Critérios Utilizados para Aferição e Auditoria de Ativos Geridos pela Gestora**

A verificação e atualização dos critérios utilizados para aferição e auditoria de ativos geridos pela Gestora consiste nos seguintes procedimentos:

- i. Verificação trimestral acerca dos critérios utilizados pelos Colaboradores do Grupo Stratus para a aferição do valor de mercado das empresas pertencentes às carteiras dos fundos geridos pela Gestora; e
- ii. Verificação anual, no contexto do processo de auditoria dos fundos geridos pelo Grupo Stratus, dos métodos, métricas e critérios de aferição empregados nas demonstrações financeiras dos fundos geridos, bem como nos demais documentos auditados pelos respectivos auditores independentes contratados, sempre procurando atender às melhores práticas de governança de fundos de investimento nacionais e internacionais.

### **8. CONTROLE DE VERSÕES**

<b>Histórico das atualizações</b>		
<b>Data</b>	<b>Versão</b>	<b>Responsável</b>
Junho/2016	1ª	Diretor de Compliance
Novembro/2021	2ª	Diretor de Compliance
Junho/2022	3ª e atual	Diretor de Compliance

\*\*\*

## **ANEXO 1.5 – TERMO DE ADESÃO AO CÓDIGO**

### **Termo de Adesão**

Declaro que tomei conhecimento do inteiro teor do Manual de Regras, Procedimentos e Descrição dos Controles Internos do Grupo Stratus (“Manual”), com o qual estou de acordo e ao qual confirmo minha adesão, comprometo-me a cumpri-lo de forma ativa na minha condição de colaborador do Grupo Stratus. Declaro também que tenho conhecimento que o Manual poderá sofrer revisões e atualizações periódicas, sendo certo que se manterão os efeitos da presente adesão às suas novas versões caso eu não informe por escrito a respeito de minha não concordância e adesão às novas versões do Manual.

Data:

Assinatura do colaborador:

Nome do colaborador:

RG:

CPF:

Assinatura do representante da empresa do Grupo Stratus:

**ANEXO 3.3 – Modelo de Compromisso de Confidencialidade**

Ao Grupo Stratus

**REF.: COMPROMISSO DE CONFIDENCIALIDADE**

Prezados,

Considerando que:

- a) a Stratus Investimentos Ltda. (“Administradora”) em conjunto com a Stratus Gestão de Carteiras Ltda. (“Gestora”) e com quaisquer outras empresas que sejam ou venham ser suas controladoras, controladas, coligadas ou estejam sob controle comum (“Grupo Stratus”) desenvolvem negócios de administração de carteiras de valores mobiliários com foco estratégico em ativos estruturados / fundos de participações negociadas em contexto privado (“*alternative assets*” / “*private equity*”);
- b) para desenvolver esses negócios, o Grupo Stratus tem acesso e lida com informações sobre empresas-alvo e projetos de investimento de caráter privilegiado, tais como, por exemplo, informações financeiras, comerciais e jurídicas, planos de desenvolvimento futuro;
- c) para ter acesso a essas informações, o Grupo Stratus, via de regra, se submete a Acordos de Confidencialidade junto à empresa-alvo ou empreendedor proprietário do projeto de investimento;
- d) eu poderei ter acesso a informações de que o Grupo Stratus dispõe sobre as empresas-alvo, investidores, projetos de investimento e clientes do Grupo Stratus, por meio de:  
(a) documentos e informações sigilosas disponíveis, incluindo mas não se limitando através da rede de computadores do Grupo Stratus; (b) pelo contato com clientes e colaboradores do Grupo Stratus; (c) acesso às dependências do Grupo Stratus, ou (d) por qualquer outro meio;

Obrigo-me a consultar e obter autorização prévia do Grupo Stratus, por escrito, antes de fazer qualquer declaração ou fornecer quaisquer informações a quaisquer terceiros, na forma escrita, verbal, eletrônica, ou em qualquer outra forma, que diga(m) respeito aos negócios, clientes ou investidores do Grupo Stratus, independentemente da sua viabilização ou não, incluindo, mas não limitado a informações relativas a: (i) empresas-alvo / empresas investidas por fundos administrados e/ou geridos pelo Grupo Stratus / projetos de investimento; (ii) transações em estudo ou em andamento, bem como o teor das discussões ou negociações desenvolvidas, (iii) planos internos do próprio Grupo Stratus,. Obrigo-me ainda a não citar nomes de investidores, clientes, nem tampouco valores envolvidos nos projetos, realizados ou não, quer seja em trabalhos acadêmicos ou até mesmo currículo profissional, exceto quando obrigado por lei, ou quando tal informação já seja de domínio público.

Adicionalmente, se, por alguma razão, autoridades governamentais exigirem a revelação ou disponibilização das informações de que trata essa carta, obrigo-me a dar ciência imediata ao Grupo Stratus do ocorrido.

Assumo ainda, por um período de 5 (cinco) anos após o meu desligamento do Grupo Stratus, a obrigação de não divulgar a terceiros quaisquer informações veiculadas internamente ao Grupo Stratus, salvo mediante autorização prévia e por escrito do Grupo Stratus.

Atenciosamente.

Data:

Assinatura do colaborador:

Nome do colaborador:

RG:

CPF: