POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

AURUM GESTÃO DE PATRIMÔNIO LTDA.

Janeiro/2024

ÍNDICE

POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

Razão Social: Aurum Gestão de Patrimônio Ltda. ("Aurum" ou, simplesmente, "Gestora")
CNPJ/MF nº 33.534.220/0001-54
Site: http://www.aurumwm.com.br

PARTE A - ASPECTOS GERAIS

1. INTRODUÇÃO

A Diretoria de Compliance da Aurum é responsável pela elaboração, implementação e manutenção do programa de Compliance ("Programa de Compliance") da Gestora. O Programa de Compliance inclui regras, políticas e procedimentos ("Políticas"), que atendem a regulamentações vigentes, processos referentes à revisão e atualização periódica das políticas e códigos constantes deste manual ("Revisão Periódica"), implementação de controles internos e testes de aderência ("Controles") para monitorar a efetividade das Políticas, e condições de realização de treinamentos aos sócios e colaboradores ("Treinamento").

O Programa de Compliance da Aurum foi desenvolvido a fim de cumprir as obrigações estabelecidas nas normas da Comissão de Valores Mobiliários ("CVM"), especialmente a Resolução CVM nº 50/21, a Resolução CVM nº 21/21 e a Resolução CVM nº 175/22e nas normas da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") às quais a Aurum seja aderente, especialmente o Código de Administração de Recursos de Terceiros ("Código de Administração de Recursos de Terceiros").

2. GOVERNANÇA

A. Comitê de Risco, Compliance e PLD

A Aurum conta com um Comitê de Risco, Compliance e PLD com autonomia sobre as questões de Compliance da mesma. Seguem abaixo as características deste Comitê:

Competência: Entre outras competências, este Comitê é responsável pela análise e revisão dos limites e o enquadramento das carteiras de valores mobiliários sob gestão; criação, revisão e cumprimento de regras, políticas, procedimentos e controles internos; e o acompanhamento de questões regulatórias, autorregulatórias e legislações do

mercado de capitais. Adicionalmente, o Comitê visa a apurar e tomar determinadas decisões e aprovações de Compliance, quanto à Prevenção à Lavagem de Dinheiro, ao ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("PLD"). Por fim, o Comitê também pode tratar a respeito de assuntos sobre Cibersegurança.

Composição: Diretor de Gestão, Diretor de Risco, Compliance e PLD e pela Equipe de gestão e Analista de RI.

Frequência: Mensal ou quando for necessário.

Decisões: As decisões do Comitê de Risco, Compliance e PLD são tomadas pelo voto da maioria dos seus membros e deverão ter o voto favorável do Diretor de Risco, Compliance e PLD, a quem sempre será garantido o poder final de decisão em matérias de gestão de Compliance. Em relação a medidas corretivas e medidas emergenciais, o Diretor de Compliance poderá decidir monocraticamente, sujeito à ratificação do Comitê.

Forma de registro das decisões: Registro em ata, as quais deverão ser assinadas pelos membros presentes à reunião, devendo permanecer arquivadas na sede da Gestora.

B. Diretoria de Compliance

Competência: A Diretoria de Compliance da Aurum tem competência para:

- Assegurar que os colaboradores, sócios e prestadores de serviços, ajam de acordo com os melhores interesses dos investidores e com integridade em relação ao mercado;

- Evitar a prática de condutas que possam afetar ou prejudicar a imagem da Aurum, dos seus sócios e colaboradores, e dos mercados financeiros e de capitais;

- Prestar ativamente assessoria aos sócios e colaboradores em relação a assuntos regulatórios e promover continuamente a cultura de ética e Compliance; e

- Administrar o relacionamento com agentes fiscalizadores, reguladores e de autorregulação.

Garantia de independência: A Diretoria de Compliance da Aurum é independente, podendo empregar seus poderes com relação à qualquer sócio ou colaborador da Gestora. Não obstante, a Diretoria de Compliance transmite reportes periódicos ao Comitê Executivo.

Por fim, apesar da existência da área de Compliance, os sócios e colaboradores da Aurum devem sempre agir de forma diligente e de acordo com as melhores práticas.

C. Diretor responsável pela diretoria de Compliance ("Diretor de Compliance")

Antonio Carlos da Rocha Conceição é o diretor responsável pela Diretoria de Compliance na Aurum, o que inclui a responsabilidade pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos no Artigo 25 da Resolução CVM nº 21/21. Por fim, ele também acumula a função de diretor responsável pelo risco ("Diretor de Risco") e controles internos que visam o combate e a prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("Diretor de PLD").

Na execução das atividades sob sua responsabilidade estabelecidas nesta política, o Diretor de Compliance poderá se utilizar de sistemas eletrônicos e/ou serviços de advogados ou firmas de consultoria de Compliance para suporte e auxílio em suas funções.

O Diretor de Compliance tem a responsabilidade pelo cumprimento desta Política. Nos casos em que entender que haja fundada suspeita em dissonância com o previsto nesta Política, deve submeter estes a apreciação do Comitê de Risco, Compliance e PLD, para que sejam tomadas as medidas cabíveis.

O Comitê de Risco, Compliance e PLD e a Diretoria de Compliance são independentes das outras áreas da Aurum e poderão exercer seus poderes em relação a qualquer sócio ou colaborador.

3. CRIAÇÃO, REVISÃO E CUMPRIMENTO DE REGRAS, POLÍTICAS, PROCEDIMENTOS E CONTROLES INTERNOS

Para que a Aurum mantenha as melhores práticas e cumpra os requisitos legais e regulatórios, é de responsabilidade da Diretoria de Compliance a criação de um Programa de Compliance ("Programa") que compreenda as seguintes regras, políticas, procedimentos e controles internos:

- Política de Compliance e Controles Internos, incluindo:
    - Política de prevenção de conflitos de interesse;
    - Política de negociações da gestora;
    - Política de confidencialidade e segurança de informações;

- Política de contratação de terceiros; e
- Política de treinamento de colaboradores.

- Código de Ética e Padrões de Conduta Profissional, incluindo;
  - Política de presentes e diversões;
  - Política de segregação de atividades e/ou de áreas;
- Política de Combate ao Suborno e Corrupção;
- Política de Investimentos Pessoais;
- Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa; e
- Política Operacionais, incluindo:
  - Política de voto;
  - Política de rateio de ordens; e
  - Política de certificação.

É de responsabilidade da Diretoria de Compliance a supervisão do cumprimento deste Programa pelos sócios, colaboradores e prestadores de serviços contratados da Aurum. Adicionalmente, a Diretoria de Compliance também é responsável pela elaboração do relatório de conclusão de controles internos de que trata o Artigo 25 da Resolução CVM nº 21/21 ("Relatório Anual de Compliance"), o qual deverá ser entregue à administração da Gestora até o último dia útil de abril de cada ano, referente aos processos de Compliance verificados no ano-civil imediatamente anterior. O Relatório Anual de Compliance deverá ser arquivado na sede da Aurum, permanecendo disponível para eventual consulta pela CVM.

Ao menos uma vez por ano, a Diretoria de Compliance deverá conduzir uma revisão completa de todo o Programa de Compliance.

4. DISPONIBILIZAÇÃO DA POLÍTICA

Em cumprimento ao Inciso III do Artigo 16 da Resolução CVM nº 21/21, a presente Política de Compliance e Controles Internos está disponível no seguinte endereço eletrônico:

http://www.aurumwm.com.br

Adicionalmente, a mesma Política também está disponível na intranet da Gestora através do endereço abaixo para o acesso de todos os seus sócios e colaboradores.

Z:\Manuais & Políticas\Vigentes

5. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e será alterada quando necessário e sem aviso prévio. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência. As alterações serão divulgadas a todos os sócios e colaboradores da Aurum pela Diretoria de Compliance e ficarão disponíveis para consulta de qualquer sócio e colaborador na intranet e no website da Aurum acima indicados.

PARTE B - CONFLITOS DE INTERESSES

É de responsabilidade da Diretoria de Compliance o cumprimento do que está disposto na presente Política e no Código de Ética e Padrões de Conduta Profissional e demais políticas da Aurum, no que tange a administração de eventuais conflitos de interesses, reais e potenciais.

Deste modo é de responsabilidade da Diretoria de Compliance deliberar e recomendar eventuais sanções aos sócios e colaboradores da Aurum sobre situações que possam ser caracterizadas como de conflitos de interesses, tanto pessoais como profissionais. Esses conflitos podem acontecer, inclusive, mas não se limitando, às seguintes situações endereçadas em políticas próprias: investimentos pessoais, atividades externas, presentes e entretenimentos, contribuições políticas, transações com partes relacionadas, contratação de fornecedores ou prestadores de serviços que tenham vínculo com partes relacionadas, alocações de oportunidades e despesas entre veículos geridos, dentre outros exemplos.

1. ASPECTOS GERAIS

A. Definição

Conflitos de interesses são todas as circunstâncias em que relacionamentos ou fatos relacionados aos interesses pessoais puderem interferir na objetividade e isenção necessária na forma de atuação Gestora, tornando os negócios incompatíveis.

B. Exemplos

São exemplos de conflitos de interesses as situações ou fatos em que há:

- Influência quanto ao julgamento do colaborador atuando em nome da Gestora;
- Desvio de oportunidades de negócios da Gestora;
- Concorrência com a atividade/negócio da Gestora;
- Ocupação significativa do tempo ou da atenção dispensada pelo colaborador, diminuindo sua eficiência e produtividade em relação às suas tarefas profissionais;
- Prejuízo à reputação do colaborador ou à imagem da Gestora; e
- Caracterização de benefícios exclusivos ao colaborador às expensas da Gestora.

C. Dever de prevenir

O colaborador deve evitar a existência de conflitos de interesse, além de atentar cuidadosamente para situações envolvendo familiares ou parentes.

D. Dever de informar

A Gestora preocupa-se em evitar circunstâncias que possam produzir conflito de interesses, seja em situação de colisão de interesses da Gestora com os dos colaboradores, seja com os dos clientes.

As eventuais situações de conflito de interesses ou potenciais conflitos de interesses verificadas pelos sócios ou colaboradores deverão ser reportadas a Diretoria de Compliance mediante envio de e-mail ao diretor de Compliance que tratará o reporte, juntamente com a Diretoria de Compliance, de forma sigilosa.

Em caso de dúvida, o potencial conflito de interesse deverá ser levado ao conhecimento do Comitê de Risco, Compliance e PLD, que definirá a linha de ação a ser tomada.

Por fim, a Aurum entende necessário também acompanhar e evitar eventuais conflitos de interesses entre o desempenho da atividade de administração de carteiras e atividades desenvolvidas por outras empresas pertencentes a seu grupo. Desta forma, com a preocupação de manter o maior nível de isenção na condução de seus negócios, na hipótese de originação de oportunidades de negócio à Aurum por qualquer empresa a ela relacionada, o cliente deverá ser informado sobre o relacionamento entre as duas empresas, bem como sobre possível situação de conflito de interesses no caso, respeitadas as previsões normativas específicas.

2. INFORMAÇÃO PRIVILEGIADA

A. Definição

Informação privilegiada ("*insider information*") é definida como aquela que não é de domínio público e que tenha impacto material na avaliação dos ativos de um determinado emissor, ou conjunto de emissores ou do mercado em geral, e que foi obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

Exemplos de informações privilegiadas são informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO).

B. Vedações

É vedado aos sócios e colaboradores qualquer tipo de operação em mercado financeiro, que seja realizada de posse de informação privilegiada, seja esta operação para benefício dos fundos geridos, seja para investimentos pessoais. Além disso, é vedada a comunicação de informação privilegiada a terceiros.

C. Dever de comunicar

Caso os sócios e colaboradores tenham acesso, por qualquer meio, a informação privilegiada, deverão levar tal circunstância ao imediato conhecimento da Diretoria de Compliance, indicando, além disso, a fonte da informação privilegiada assim obtida. Tal dever de comunicação também será aplicável nos casos em que a informação privilegiada seja conhecida de forma acidental, em virtude de comentários casuais ou

por negligência ou indiscrição das pessoas obrigadas a guardar segredo. A Gestora mantém registro de reuniões externas com *asset managers*.

3. MANIPULAÇÃO DE MERCADO

A. Definição

São definidas como "Manipulação de Mercado" as práticas ou dispositivos que, mesmo que potencialmente, interfiram no correto funcionamento do mercado de valores mobiliários. São proibidas, nos termos da Instrução CVM nº 8/79 quatro tipos principais de infrações:

- Criação de condições artificiais de demanda: condições criadas em decorrência de negociações pelas quais seus participantes ou intermediários, por ação ou omissão dolosa provocarem, direta ou indiretamente, alterações no fluxo de ordens de compra ou venda de valores mobiliários;

- Manipulação de preços no mercado de valores mobiliários: a utilização de qualquer processo ou artifício destinado, direta ou indiretamente, a elevar, manter ou baixar a cotação de um valor mobiliário, induzindo, terceiros à sua compra e venda;

- Operação fraudulenta no mercado de valores mobiliários: operação em que se utilize ardil ou artifício destinado a induzir ou manter terceiros em erro, com a finalidade de se obter vantagem ilícita de natureza patrimonial para as partes na operação, para o intermediário ou para terceiros; e

- Prática não equitativa no mercado de valores mobiliários: prática de que resulte, direta ou indiretamente, efetiva ou potencialmente, um tratamento para qualquer das partes, em negociações com valores mobiliários, que a coloque em uma indevida posição de desequilíbrio ou desigualdade em face dos demais participantes da operação.

B. Tipos

Entre as formas de Manipulação de Mercado catalogadas, encontram-se as seguintes práticas:

- "Zé-com-zé" ("*Wash Trades*"): comprar e vender a mesma ação de modo a mover os preços praticados nos mercados;

- "*Pools*": acordos dentro de um mesmo grupo de traders para delegar a um gestor os poderes para negociar uma ação específica por um período determinado de tempo;

- "*Churning*": entrar com ordens de compra e venda no mesmo preço, a fim de auferir taxas de corretagem através de negociação excessiva;

- "*Stock Bashing*" ou "*Pump and Dump*": fabricar informações falsas ou enganosas sobre um ativo com o objetivo de aumentar ou deprimir o preço, e realizar uma venda ou uma compra após a mudança de preço;

- "*Bear Raid*": vender a descoberto uma ação e utilizar informações negativas para conseguir ganhos de curto prazo;

- "*Lure and Squeeze*": vender ação de empresa em problemas com o conhecimento de que tal empresa utilizará ações para solucionar sua situação com credores.

C. Ações preventivas e integridade do processo de investimento

Como forma de proteção, a Gestora também busca preservar a integridade do processo de investimento de modo a garantir que decisões de compra e venda de ativos sejam baseadas em análises aprofundadas e que sejam devidamente registradas e documentadas por evidências. São dois os tipos de integridade:

- Integridade em investimentos de longo prazo, baseada na análise fundamentalista de ativos; e

- Integridade na análise, baseada em material original ou proprietário produzido pela própria Gestora, processo endógeno de obtenção de informações sobre ativos e companhias, e proteção de informações privilegiadas.

D. Mecanismos de proteção

A Gestora utiliza-se dos seguintes mecanismos específicos de prevenção de manipulação:

- Controle de fluxos de informações;

- Monitoramento de traders e centralização das ordens em nome da Aurum;

- Detecção de atividades suspeitas e atividades de risco;

- Treinamento e orientação de colaboradores; e

- Política de negociações pessoais restritivas, com *disclosure* mandatório de operações.

4. TRATAMENTO DE EVENTUAIS CONFLITOS DE INTERESSES COM EMPRESAS DO GRUPO

O tratamento dos eventuais conflitos de interesses entre as atividades prestadas pela Aurum e as empresas do grupo, bem como as segregações existentes entre a Aurum e as demais empresas do grupo estão sendo abordados na Parte H – "Conflito de Interesses e Segregação de Atividades e/ou de Áreas" do Código de Ética e Padrões de Conduta Profissional da Aurum.

PARTE C - POLÍTICA DE CONFIDENCIALIDADE

1. ASPECTOS GERAIS

A. OBJETO

Esta política tem por escopo proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme o Parágrafo 8º do Artigo 4º e inciso II do Artigo 28 da Resolução CVM nº 21/21.

Confidencialidade é um princípio fundamental e aplica-se a quaisquer informações não-públicas referentes aos negócios da Aurum, como também a informações recebidas de seus clientes, contrapartes ou fornecedores da Aurum durante o processo natural de condução de negócios. Os colaboradores não devem transmitir nenhuma informação não-pública a terceiros.

Deste modo, nenhuma informação considerada sigilosa deve ser divulgada, dentro ou fora da Aurum, para pessoas que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Adicionalmente, qualquer informação sobre a Aurum, ou de qualquer natureza relativa as suas atividades ou a de seus sócios, colaboradores e clientes só poderá ser fornecida ao público, mídia ou a demais órgãos, caso autorizado pela Diretoria de Compliance.

B. RESPONSABILIDADE

É de responsabilidade da Diretoria de Compliance o controle da disseminação de informações confidenciais. Informações confidenciais e/ou privilegiadas só podem ser

repassadas a outras áreas e terceiros, que não tinham acesso a tais, com a prévia autorização da Diretoria de Compliance. Adicionalmente é de responsabilidade da Diretoria de Compliance supervisionar o cumprimento das regras de disseminação de informações confidenciais por meio do monitoramento dos sócios e colaboradores quanto aos meios de comunicação.

A Diretoria de Compliance tem a responsabilidade pela implementação e monitoramento desta política. Todos os colaboradores da Aurum têm o dever de:

- Obedecer a política de segurança da informação;
- Proteger informações sigilosas contra o acesso, modificação, destruição ou divulgação não autorizada pela Aurum;
- Seguir as leis e normas que regulamentam os aspectos relacionados à propriedade intelectual no que se refere às informações sigilosas;
- Assegurar que os recursos da Aurum a sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela mesma;
- Buscar orientação do superior hierárquico em caso de dúvidas relacionadas a segurança das informações sigilosas; e
- Comunicar imediatamente a Diretoria de Compliance a respeito de qualquer descumprimento ou violação da política de confidencialidade e/ou da política de segurança da informação.

2. DIRETRIZES

A. COMPORTAMENTO SEGURO

Os sócios e colaboradores da Aurum deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, 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.

Os sócios e colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

O disposto no presente capítulo deve ser observado durante a vigência do relacionamento profissional do colaborador com a Aurum e também após seu término

Todos os sócios e colaboradores da Aurum têm o dever de adotar a postura de comportamento seguro, que consiste nos seguintes itens:

- Assumir atitude proativa e engajada a respeito da proteção de informações consideradas sigilosas;

- Compreender as ameaças externas que podem afetar a segurança das informações sigilosas, tais como ataques de vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos e etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e servidores;

- Não discutir assuntos relacionados à Aurum e ao desempenho de suas atividades em ambientes públicos ou áreas expostas;

- Não transferir, compartilhar ou divulgar a terceiros as senhas de acesso a sistemas da Aurum;

- Não anotar em papel ou em sistemas visíveis as senhas de acesso a sistemas da Aurum;

- Bloquear seus computadores sempre que ausentarem das estações de trabalho;

- Não instalar softwares nas estações de trabalho da Aurum que não foram homologados ou previamente aprovados pela Diretoria de Compliance;

- Não abrir arquivos eletrônicos ou mensagens de e-mail de origem desconhecida;

- Não reproduzir ou disseminar dados da rede de computadores da Aurum; e

- Utilizar o e-mail corporativo e aplicativos de mensagens exclusivamente para assuntos relacionados aos negócios conduzidos pela Aurum ou para o desempenho de suas atividades.

B. POLÍTICAS GERAIS

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Aurum são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na Aurum e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os sócios e colaboradores tiverem com relação aos clientes da Aurum deve ser mantida na mais estrita confidencialidade, não podendo ser

divulgada sem o prévio e expresso consentimento do cliente, salvo na hipótese de decisão judicial específica que determine à Aurum a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da CVM. Caso a Aurum ou qualquer dos sócios e colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser seguido de imediata e expressa comunicação aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os sócios e colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Aurum, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Aurum. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da Aurum, para que sejam tomadas as medidas cabíveis.

A Aurum exige que seus sócios e colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Aurum, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Aurum, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do sócio ou colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo sócio e colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

A Aurum concederá autorização para acesso a informações e arquivos apenas que se refiram ao departamento no qual o colaborador atua. Aos sócios e colaboradores que atuem diretamente na atividade de administração de recursos, haverá além da segregação de acesso por departamento, a concessão de acesso específico para as informações do cliente e/ou do projeto sob responsabilidade de referido sócio ou colaborador.

i. *Insider Trading* e "Dicas"

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).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de informação confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

ii. *Front-running*

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 a Gestora, 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.

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 no Código de Ética e Padrões de Conduta Profissional e na legislação aplicável, incluindo eventual demissão por justa causa.

PARTE D - POLÍTICA DE CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

1. ASPECTOS GERAIS

A. OBJETO

Esta política em conjunto com a Política de Confidencialidade acima descrita, tem como finalidade proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme o Parágrafo 8º do Artigo 4º da Resolução CVM nº 21/21, o Código de Administração de Recursos de Terceiros e o Guia de Cibersegurança elaborado pela ANBIMA.

B. RESPONSABILIDADE

Como a Aurum se utiliza de um prestador de serviço contratado para administrar a sua área de Tecnologia da Informação - TI, é de responsabilidade da Diretoria de Compliance o gerenciamento e controle de qualidade do serviço prestado por este.

Sendo assim, a Diretoria de Compliance tem através do terceiro contratado a responsabilidade pela implementação e monitoramento desta política, considerando os assuntos abaixo:

- Identificação e avaliação de riscos;
- Ações de prevenção e proteção;
- Monitoramento e testes;
- Criação de um plano de resposta; e
- Reciclagem e revisão.

2. DIRETRIZES

A. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A Aurum, como uma gestora de recursos independente, conta com um servidor de processamento de dados, um servidor de armazenamento de dados e computadores individuais para todos os seus colaboradores para executar todas as suas funções. Adicionalmente, a Aurum conta com uma Intranet desenvolvida para armazenar programas e dados, acesso a internet para os seus computadores e servidores e telefones com um servidor dedicado para a gravação de dados para esses últimos aparelhos.

Dado o tamanho diminuto da Aurum, toda a informação e dado administrado por ela é considerado como confidencial e, logo, a Política de Confidencialidade e a Política de Segurança de Informações se aplica a todos esses.

Adicionalmente, com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, a Aurum tomou a decisão conservadora de restringir o uso de sua infraestrutura apenas ao exercício de sua função, o que auxilia na prevenção e diminuição de ataques e ameaças cibernéticas.

Em casos de identificação de ataques e ameaças por parte de seus sócios e colaboradores, a Aurum pede que esses sejam reportados conjuntamente para a Diretoria de Compliance e para a empresa tercerizada responsável por TI. Esses casos depois são reportados no Comitê de Risco, Compliance e PLD.

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

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);

- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- 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 Gestora 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.

B. AÇÕES DE PREVENÇÃO E PROTEÇÃO

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados, cujo acesso é permitido apenas aos administradores da Aurum, além dos membros do departamento de informática.

Todo software disponibilizado aos sócios e colaboradores deverá ser utilizado somente para os negócios da Aurum, em consonância com os acordos de licenciamento firmados.

É realizado back up de todas as informações e armazenadas em nuvem, em um HD externo e no CPD com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O processo de back-up é realizado da seguinte maneira:

- Banco de Dados: O back-up do banco de dados dos sistemas utilizados pela Aurum é realizado diariamente por esta, com retenção de 30 dias nos servidores da própria Aurum. Adicionalmente, há um processo diário com retenção em nuvem dos últimos 5 anos e que pode ser acessado remotamente. Por fim, existe também um hard drive externo que realiza o back-up diário dos dados do servidor e fica localizado nos servidores da Aurum.

- E-mail: O back-up dos dados de e-mail utilizados pela Aurum é de responsabilidade da Microsoft, feito em nuvem e hospedado nos servidores desta.

- Telefonia: O back-up dos dados de telefonia utilizados pela Aurum é realizado diariamente, com retenção de 30 dias nos servidores da Aurum. Adicionalmente, há um processo diário com retenção em nuvem dos últimos 5 anos.

O acesso aos sistemas de informação da Aurum é feito por meio de um par "usuário/senha" que permite ao responsável pelo departamento de informática acompanhar, de forma precisa as atividades desenvolvidas por cada um dos colaboradores. O controle desses dados é de domínio da Aurum, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

Todos os acessos concedidos são avaliados conforme o envolvimento de cada colaborador com clientes e/ou projetos específicos. Desta forma, a concessão de acesso às informações obtidas para o exercício da atividade de administração observará dois critérios:

- Acesso restrito apenas aos colaboradores envolvidos com a atividade de administração de carteiras, sendo, portanto, inacessíveis aos colaboradores de áreas administrativas da Aurum; e

- Dentre os colaboradores atuantes na área de administração de recursos, o acesso às informações será limitado apenas aos colaboradores que efetivamente atuem com determinado cliente e/ou projeto, de forma que apenas terão acesso às informações os colaboradores estritamente necessários para o desempenho da atividade em questão.

Para tanto, serão criados nos servidores próprios ou na nuvem diretórios específicos, a partir dos quais será possível controlar a concessão de acessos de acordo com as regras estabelecidas.

Todo sócio ou colaborador que tiver acesso aos sistemas de informação da Aurum é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O sócio ou colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

Adicionalmente, todos os servidores e computadores da Aurum possuem filtro de e-mail Exchange Online Protection do serviço Office 365 da Microsoft, Firewalls Sophos XG 135W com sistema Sophos Intercept-X operando de forma redundante e sistema antivirus Sophos Endpoint Protection Advanced.

A Aurum se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Aurum ou utilizados em nome dela, a fim de assegurar o fiel cumprimento deste Manual, bem como da legislação em vigor.

C. COMUNICAÇÕES

i. Internet

Todos os sócios e colaboradores da Aurum têm o dever de utilizar a internet exclusivamente para assuntos relacionados aos negócios conduzidos pela Aurum ou para o desempenho de suas atividades. O acesso a internet é monitorado permanentemente e os arquivos contendo os registros dos acessos e das tentativas de acesso são armazenadas pela Aurum, sendo que a Diretoria de Compliance é informada sobre estes acessos e tentativas de acesso.

ii. Telefone

Todos os sócios e colaboradores da Aurum tem o dever de utilizar o sistema de telefonia exclusivamente para assuntos relacionados aos negócios conduzidos pela Aurum ou para o desempenho de suas atividades. O sistema de telefonia é monitorado e gravado pela Aurum, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iii. Aplicativos de mensagem

Todos os sócios e colaboradores da Aurum tem o dever de utilizar os aplicativos de mensagens exclusivamente para assuntos relacionados aos negócios conduzidos pela Aurum ou para o desempenho de suas atividades. Os aplicativos de mensagens são monitorados e gravados pela Aurum, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iv. Mídias externas e/ou portáteis

Todos os sócios e colaboradores da Aurum são proibidos de utilizar mídias externas e/ou portáteis para transferir dados, sistemas e arquivos da rede da Aurum.

Para utilização destes equipamentos, os sócios e colaboradores devem solicitar a Diretoria de Compliance para efetuar esta atividade, dado que apenas esta diretoria tem acesso a este tipo de equipamento. Adicionalmente, esta solicitação precisa ser relacionada aos negócios conduzidos pela Aurum ou para o desempenho das atividades do requisitante.

D. ACESSO AOS RECURSOS

i. Acesso Remoto

Para utilização de aplicativos/programas de acesso remoto, os sócios e colaboradores devem solicitar autorização da Diretoria de Compliance.

ii. Utilização de recursos

Todos os sócios e colaboradores da Aurum têm o dever de não utilizar os recursos disponibilizados pela Aurum como de uso pessoal.

Conforme mencionado neste capítulo, a utilização dos recursos disponibilizados pela Aurum está sujeita ao monitoramento periódico, sem frequência determinada ou aviso prévio. Adicionalmente, os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto da política de

segurança da informação e demais regras internas da Aurum, e, conforme o caso servir como evidência em processos administrativos e/ou legais.

E. TESTES PERIÓDICOS

Periodicamente, a Aurum realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- Verificação do login dos colaboradores;
- Anualmente, altera-se a senha de acesso dos colaboradores;
- Testes no *firewall*;
- Testes nas restrições impostas aos diretórios;
- Manutenção trimestral de todo o *hardware* por empresa especializada em consultoria de tecnologia de informação;
- Manutenção trimestral com a atualização de todo o *software* pela empresa especializada em consultoria de tecnologia de informação; e
- Testes no back-up (salvamento de informações) diário, realizado na nuvem, HD externo e no próprio CPD da Aurum.

F. CRIAÇÃO DE UM PLANO DE RESPOSTA

No caso de um eventual ciberataque, o procedimento a ser adotado depende do grau de severidade do ataque sofrido:

- Utilização comprometida de um ou mais computadores: Os sócios e colaboradores afetados tem o dever de reportar o problema para a Diretoria de Compliance e conjunto com a empresa tercerizada responsável por TI. Nesse caso, a empresa de TI tem o dever de tentar reparrar o prejuízo causado e o sócio ou colaborador prejudicado, pode trabalhar de um computador notebook ou outro computador desktop sem utilização que a Aurum possui; e
- Utilização comprometida de toda a intranet e/ou de todos os computadores: Os sócios e colaboradores afetados tem o dever de reportar o problema para a Diretoria de Compliance e conjunto com a empresa tercerizada responsável por TI. Nesse

caso, a empresa de TI tem o dever de tentar reparrar o prejuízo causado e a Política de Contingência e de Continuidade de Negócios é acionada.

G RECICLAGEM E REVISÃO

A Diretoria de Compliance em conjunto com a empresa responsável por TI ficam incubidas de produzirem um relatório toda vez que cibersegurança da Aurum for comprometida. Esse relatório é apresentado no Comitê de Risco, Compliance e PLD e contempla os danos incorridos e as ações tomadas e sugestões para melhora com relação ao procedimento.

PARTE E - POLÍTICA DE CONTRATAÇÃO DE TERCEIROS

1. CRITÉRIOS DE CONTRATAÇÃO

A Gestora pode contratar terceiros para a prestação de determinados serviços relacionados ao objeto social da Gestora, sempre que permitido pela legislação ou regulamentação aplicáveis ao exercício de sua atividade.

Para fins da contratação de terceiros, a Gestora observa os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade do terceiro contratado. A aferição destas condições é realizada através da análise de documentação, e eventual realização de visitas, bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do terceiro contratado. A contratação de futuros prestadores pela Gestora considera a qualificação adequada para cada posição a ser ocupada, e avalia não somente a formação técnica dos candidatos, mas também suas experiências em trabalhos anteriores.

A Aurum, no limite da sua responsabilidade enquanto empregadora ou tomadora de serviços, a depender da situação fática, implementa todos os procedimentos necessários ao monitoramento das atividades prestadas por seus sócios, colaboradores e prestadores de serviço contratados, sempre balizado no princípio da eficiência, transparência e boa-fé, nos termos da legislação e da regulamentação vigente.

2. DUE DILIGENCE & PROCESSO DE CONTRATAÇÃO

Quando da eventual contratação de prestadores de serviço pela Aurum, nas hipóteses em que a legislação e/ou a regulamentação permitir, o terceiro deve observar os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade. A aferição destas condições é realizada através da análise de documentação, e eventual realização de visitas (*due dilligence*), bem como quaisquer outros procedimentos que

sejam julgados necessários para comprovar as qualificações do prestador de serviços contratado. Quando for o caso, o potencial candidato também deve submeter a análise da Aurum o questionário ANBIMA de Due Diligence específico para a atividade contratada, e sua Política de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo.

O processo de contratação e supervisão do terceiro deve ser sempre efetuado visando o melhor interesse de seus clientes, especialmente em casos em que haja ligação direta ou indireta entre a Gestora e a empresa contratada ou em hipóteses de potenciais conflitos de interesse. Adicionalmente, é dever da Aurum sempre fornecer aos seus investidores total transparência com relação a eventuais recebimentos de serviços contratados ou relacionamento, como no caso da contratação de Corretoras.

É de responsabilidade da Diretoria de Compliance que esta esteja envolvida na diligência de potenciais fornecedores e prestadores de serviços, durante o processo de contratação desses. Sendo assim, durante esse procedimento, a Diretoria de Compliance deve procurar por processos, condenações e notícias desabonadoras sobre esses potenciais novos fornecedores e prestadores de serviços e seus sócios e administradores.

Adicionalmente, durante o processo de contratação, a Diretoria de Compliance tem o dever de classificar o risco potencial da atividade a ser delegada a um terceiro. A classificação deve utilizar os seguintes parâmetros:

- Baixo risco;
- Médio risco; e
- Alto risco.

Baseada nessa análise de risco, a Aurum deve descrever as supervisões necessárias para cada grau de risco diferente e nenhuma dessas pode ter uma periodicidade maior que 36 (trinta e seis) meses. Além do mais, na ocorrência de fatos relevantes envolvendo o contratado ou de alteração significativa a respeito do serviço prestado em termos de qualidade e/ou performance, a Aurum também se mantém o direito de reavaliação tempestiva destes. Todos esses processos, tem o intuito de garantir que as medidas de supervisão, prevenção e mitigação sejam proporcionais aos riscos identificados. Para maiores detalhes verificar o item “6. Supervisão Baseada em Risco” abaixo.

Por fim, é dever da Diretoria de Compliance supervisionar e formalizar em um relatório as suas análises e manifestar a sua opinião/recomendação com relação a idoneidade do fornecedor e prestador de serviço contratado e a ser contratado.

3. *BEST EXECUTION*

A Gestora pode alocar recursos em fundos de investimento geridos por terceiros e pode também negociar ativos em mercado, executando ordens e operando com corretoras.

Como agente dos fundos, destarte, tem responsabilidade fiduciária de agir para conseguir, nas circunstâncias de mercado, preços e condições de execução mais favoráveis para negócios com valores mobiliários em nome de clientes e carteiras geridas por ela. Deve, deste modo, cultivar transparência e franqueza em relação a potenciais conflitos de interesse, práticas de remuneração, benefícios indiretos, e outros fatores que possam interferir na escolha de prestador de serviço. Por essa razão, mantém política de *best execution*, buscando os melhores interesses de seus clientes.

Os objetivos da política de *best execution* são os seguintes:

- Obter, nas circunstâncias existentes de mercado, best execution;
- Prevenir conflitos de interesse e o uso dos ativos dos clientes em benefício de terceiros;
- Prevenir e evitar o envolvimento de colaboradores em situações apresentando riscos de violações de deveres fiduciários;
- Permitir a detecção de riscos potenciais de violações da política;
- Reprimir ações que criem riscos para a ética, integridade e reputação;
- Reduzir o custo de enforcement interno; e
- Orientar e treinar colaboradores para identificar, prevenir, evitar e reprimir situações de risco e violações à política.

Os deveres principais da Gestora em relação à *best execution* são os seguintes:

- Dever de considerar preços, custos, velocidade, probabilidade de execução e liquidação, tamanho, natureza de ordens e quaisquer outros elementos relevantes para a estratégia;
- Dever de colocar os interesses dos clientes acima de seus próprios;
- Dever de minimizar o risco de conflito de interesse;

- Dever de ativamente evitar transações conflitadas, arranjos de soft-dollar, e negociações paralelas sem a necessária transparência e consentimento do interessado; e

- Dever de reverter todo e qualquer benefício direta ou indiretamente recebidos em relação à execução de ordens de clientes.

A política de *best execution* da Gestora é baseada em três mecanismos principais:

- Pré-autorização de corretoras baseada em critérios objetivos e rotinas de avaliação: a Gestora somente opera com corretoras pré-selecionadas com base nos seguintes critérios:

    - Capacidade de execução e habilidades da corretora (habilidade de executar trades de diferentes tamanhos, tipos e papel);

    - Confiabilidade dos sistemas de comunicação e negociação da corretora;

    - Comissões e descontos; e

    - Reputação e saúde financeira da corretora e de seu grupo financeiro.

- Revisão periódica de políticas: revisão periódica e sistemática das políticas de corretoras autorizadas; e

- Recusa de vantagens e serviços em troca de preferência de execução: A Gestora não aceita serviços que não sejam pesquisa.

Para estruturar sua política de *best execution*, a Gestora formou um comitê encarregado de realizar o direcionamento de fluxo de trade. O comitê tem poderes para: avaliar se há conflito de interesse entre a Gestora e uma contraparte, estabelecer critérios para avaliar a qualidade da execução de ordens, e realizar o acompanhamento, selecionar, avaliar e classificar corretoras e contrapartes em vista dos serviços de execução buscados e estabelecer balizas para o *trader* direcionar o fluxo de negócios. O comitê é formado pelo Diretor de Gestão, Diretor de Compliance e equipe de análise. O comitê reunir-se-á ordinariamente, trimestralmente, e extraordinariamente, quando houver necessidade.

A execução de ordens procura fazer com que as alterações de posição se dêem de maneira eficiente, com minimização de custos e execução aos preços desejados. Hoje a gestora mantém uma lista de corretoras, da qual solicita três diferentes cotações, sendo escolhida a de taxas mais baratas e maior velocidade de execução. As ordens podem ser colocadas por telefone ou sistema eletrônico.

4. TRATAMENTO DE CONFLITOS DE INTERESSE

Os conflitos de interesse estão ligados à ocorrência de situações com potencial para gerar adversidades, desentendimentos, condutas indesejáveis e oportunistas, trazendo assim consequências prejudiciais ao bom andamento dos negócios e, em casos mais graves, violações sujeitas a sanções e multas.

A Aurum em suas práticas diárias, deve avaliar a possibilidade de ocorrerem situações de conflito de interesse, dando especial atenção às transações e situações que, em face de sua natureza, forma a identidade das partes, possam ser consideradas controversas ou que possam representar efetivo ou potencial conflito de interesses.

5. CONTRATAÇÃO

O início das atividades do prestador deve ser vinculado à formalização da contratação, e nenhum tipo de pagamento poderá ser efetuado antes da celebração do contrato. As tratativas acerca do vínculo contratual serão conduzidas por pela Área de Compliance da Gestora.

O contrato escrito a ser celebrado deverá prever, no mínimo, cláusulas que tratam:

(a) das obrigações e deveres das partes envolvidas;

(b) da descrição das atividades que serão contratadas e exercidas por cada uma das partes;

(c) da obrigação de cumprir suas atividades em conformidade com as disposições previstas na regulamentação e autorregulação aplicáveis à atividade; e

(d) da obrigação, no limite de suas atividades, de deixar à disposição do administrador fiduciário dos fundos de investimento todos os documentos e informações que sejam necessários para a elaboração de documentos e informes periódicos exigidos pela regulação em vigor.

Quando o prestador tiver acesso a informações sigilosas dos clientes e da Gestora, deverá ser assinado um contrato com cláusula de confidencialidade que estabeleça multa em caso de quebra de sigilo, ou deverá ser firmado termo de confidencialidade, o qual deverá ser arquivado na sede da Gestora. O funcionário do prestador que tiver acesso a informações confidenciais deverá assinar pessoalmente termo de confidencialidade, comprometendo-se a guardar o sigilo das referidas informações.

Ao contratar terceiros que porventura pertençam ao seu Conglomerado ou Grupo Econômico, ou ao Conglomerado ou Grupo Econômico dos investidores dos fundos de investimento sob sua gestão, a Gestora zelará para que as operações observem condições estritamente comutativas ora estabelecidas nesta Política.

Para fins desta Política, "Conglomerado" ou "Grupo Econômico" significam um conjunto de entidades controladoras diretas ou indiretas, controladas, coligadas ou submetidas a controle comum.

6. OBRIGAÇÕES DE SELEÇÃO, ANÁLISE DE CONTRATAÇÃO DE PRESTADORES DE SERVIÇOS – RESOLUÇÃO CVM 175/22

A contratação de terceiros pela AURUM contará com prévia e criteriosa análise e seleção do contratado, devendo a AURUM, ainda, figurar no contrato como interveniente anuente.
São obrigações da AURUM em contratar, em nome do fundo, com terceiros devidamente habilitados e autorizados, os seguintes serviços:

- intermediação de operações para a carteira de ativos;
- distribuição de cotas;
- consultoria de investimentos;
- classificação de risco por agência de classificação de risco de crédito;
- formador de mercado de classe fechada;
- cogestão da carteira de ativos.

A AURUM poderá prestar os serviços de intermediação de operações para a carteira de ativos e distribuição, observada a regulamentação aplicável às referidas atividades.
Os serviços listados acima somente são de contratação obrigatória pela AURUM caso assim disposto no regulamento ou deliberado pela assembleia de cotistas da classe de cotas.
Nos casos de contratação de cogestor, o contrato deve definir claramente as atribuições de cada gestor, o que inclui, no mínimo, o mercado específico de atuação de cada gestor e a classe ou classes de cotas objeto da cogestão.
Ainda, a AURUM poderá contratar outros serviços em benefício da classe de cotas, que não estejam listados acima, observado que, nesse caso:

- a contratação não ocorre em nome do fundo, salvo previsão no regulamento ou aprovação em assembleia; e
- caso o prestador de serviço contratado não seja um participante de mercado regulado pela CVM ou o serviço prestado ao fundo não se encontre dentro da esfera de atuação da Autarquia, o gestor deve fiscalizar as atividades do terceiro contratado relacionadas ao fundo.
- Em caso o fundo contrate agência de classificação de risco de crédito:

- o contrato deve conter cláusula obrigando a agência de classificação de risco de crédito a divulgar, imediatamente, em sua página na rede mundial de computadores e comunicar à CVM, ao gestor e ao administrador qualquer alteração da classificação, ou a rescisão do contrato;
- na hipótese de que trata o item acima, a AURUM acompanhará a comunicação do fato relevante a ser realizada pelo administrador e
- as informações fornecidas à agência de classificação de risco de crédito devem abranger, no mínimo, aquelas fornecidas aos cotistas.

A rescisão do contrato firmado com agência de classificação de risco de crédito somente é admitida mediante a observância de período de carência de 180 (cento e oitenta) dias, sendo obrigatória a apresentação, ao final desse período, de relatório de classificação de risco elaborado pela mesma agência.
Caso a rescisão do contrato firmado com agência de classificação de risco de crédito ocorra por deliberação da assembleia de cotistas, o prazo será de 90 (noventa) dias.
A AURUM cumprirá e zelará para que as despesas com a contratação de terceiros prestadores de serviços que não constituam encargos do fundo não excedam o montante total, conforme o caso da taxa de administração ou de gestão, conforme estabelecida no regulamento, correndo o pagamento de qualquer despesa que ultrapasse esse limite às expensas da AURUM que a contratou.

7. CADASTRO

O prestador de serviço que for aprovado, de acordo com os requisitos estabelecidos nos itens anteriores, deve fornecer a documentação abaixo:

- Breve informação sobre o histórico da empresa;
- Cópia do contrato ou estatuto social;
- Cópia da procuração, se aplicável;
- Contrato para fins de prestação do serviço à Sociedade em linha com o conteúdo mínimo exigido pelo Código ANBIMA de Administração de Recursos de Terceiros, se for o caso.

A Aurum poderá solicitar documentos e informações adicionais caso julgue necessário para fins da seleção do prestador do serviço.

8. PROCEDIMENTOS PÓS-CONTRATAÇÃO

Após a contratação do prestador, a Gestora realizará o monitoramento contínuo das atividades exercidas pelos prestadores contratados, até o término do prazo da contratação. O monitoramento será de responsabilidade do Diretor de Compliance, que poderá contar com o auxílio do diretor responsável pela área de gestão de recursos.

A análise, para fins de monitoramento, deverá considerar o objeto contratado vis a vis a entrega realizada, com ênfase nas eventuais disparidades, na tempestividade, qualidade e quantidade esperadas. Ainda, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a Gestora.

Tendo em vista a estrutura da Gestora, o processo para monitoramento contínuo do prestador contratado será conciso e objetivo. Em linhas gerais, o Diretor de Compliance contando com o auxílio do diretor responsável pela área de gestão de recursos avaliará o desempenho do prestador *versus* a expectativa e metas traçadas quando da sua contratação, a relação custo-benefício e o grau de segurança empregado nas suas tarefas. Sem prejuízo, em casos específicos, adotará controles mais rigorosos, conforme adiante detalhado na seção abaixo, a qual trata da supervisão baseada em risco para terceiros contratados.

A partir dos elementos supracitados, o Diretor de Compliance e Risco confeccionará, em periodicidade mínima anual, um relatório a ser enviado por e-mail - com confirmação de recebimento - aos demais diretores e sócios da Gestora, para fins de ciência.

Na hipótese de serem encontradas desconformidades e ressalvas, o Diretor de Compliance notificará imediatamente o prestador contratado, para que este sane a questão ou adeque a sua conduta dentro do prazo que a Gestora entender razoável, respeitando, sempre, o contrato celebrado. Caso o prestador contratado não cumpra com os termos exigidos na notificação, o Diretor de Compliance poderá proceder com a aplicação da cláusula indenizatória eventualmente prevista ou com a descontinuidade do serviço.

9. SUPERVISÃO BASEADA EM RISCO

A supervisão baseada em risco tem como objetivo destinar maior atenção aos prestadores contratados que demonstrem maior probabilidade de apresentar falhas em sua atuação ou representem potencialmente um dano maior para os investidores e para a integridade do mercado financeiro e de capitais.

Nesse sentido, a Gestora segue a metodologia abaixo para a realização de supervisão baseada em risco dos prestadores contratados:

I. Os prestadores contratados são determinados pelos seguintes graus de risco:

- “Alto Risco”. Prestadores de serviços que tiverem suas atividades autorreguladas pela ANBIMA, mas não forem associados ou aderentes aos Códigos ANBIMA (“Códigos”);

- “Médio Risco”. Prestadores de serviços que forem associados ou aderentes aos Códigos, mas que no processo de *due diligence* prévio à contratação apresentaram informações suspeitas, inconsistentes, histórico reputacional questionável, dentre outros fatores que vierem a ser definidos pelo Diretor de Compliance e Risco; e

- “Baixo Risco”. Prestadores de serviços que forem associados ou aderentes aos Códigos**;**

II. As supervisões ocorrerão da seguinte forma:

- “Alto Risco”. Com a periodicidade anual, a Gestora deverá rever o desempenho de cada prestador avaliando, entre outros aspectos:

A) Quando Corretora: (i) a qualidade das execuções fornecidas; (ii) o custo das execuções; (iii) eventuais acordos de *Soft Dollar*; (iv) potenciais conflitos de interesse; bem como (v) andamento de processos administrativos por parte da CVM e da ANBIMA; e

B) Quando Distribuidora: (i) qualidade na usabilidade da plataforma, nos serviços prestados e estabilidade da plataforma fornecida, e (ii) potenciais conflitos de interesse, bem como andamento de processos administrativos por parte da CVM e da ANBIMA.

- “Médio Risco”. A cada a cada 24 (vinte e quatro) meses, a Gestora confirmará se o prestador mantém sua associação ou adesão à ANBIMA, bem como deverá rever o desempenho de cada prestador avaliando, entre outros aspectos:

A) Quando Corretora: (i) a qualidade das execuções fornecidas; (ii) o custo das execuções; (iii) eventuais acordos de *Soft Dollar*; (iv) potenciais conflitos de interesse, e (v) eventuais alterações nos manuais e políticas do prestador; e

B) Quando Distribuidora: (i) qualidade na usabilidade da plataforma, nos serviços prestados e estabilidade da plataforma fornecida, e (ii) potenciais conflitos de interesse, bem como andamento de processos administrativos por parte da CVM e da ANBIMA.

- “Baixo Risco”. A cada a cada 36 (trinta e seis) meses, a Gestora confirmará se o prestador mantém sua associação ou adesão à ANBIMA, bem como deverá rever o desempenho de cada prestador avaliando, entre outros aspectos:

A) Quando Corretora: (i) a qualidade das execuções fornecidas; e (ii) o custo das execuções; e

B) Quando Distribuidora: qualidade na usabilidade da plataforma, nos serviços prestados e estabilidade da plataforma fornecida.

III. A Gestora reavaliará tempestivamente os Terceiros contratados, na ocorrência de qualquer fato novo que preocupe a Gestora, ou na hipótese de alteração significativa que cause dúvidas na Gestora quanto à classificação do Terceiro.

10. MANUTENÇÃO DOS ARQUIVOS

A Aurum manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

PARTE F - POLÍTICA DE TREINAMENTO

A Política de Treinamentos da Aurum tem como objetivo estabelecer as regras que orientem o treinamento dos colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas Políticas. Todos os sócios e colaboradores recebem o devido treinamento acerca de todas as políticas e procedimentos constantes deste Manual. Assim, são proporcionados aos sócios e colaboradores uma visão geral das Políticas adotadas, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

A Aurum poderá financiar, total ou parcialmente, cursos de aprimoramento profissional aos colaboradores, principalmente aos membros da equipe técnica, desde que julgue viável e interessante o conteúdo a ser lecionado. O controle e a supervisão das práticas profissionais dos colaboradores em relação à política de treinamentos é responsabilidade do Diretor de Compliance, que visará promover a aplicação conjunta da referida Política com as normas estabelecidas nas demais Políticas aprovadas nos termos do presente Manual.

Poderão ser ministradas a todos os sócios e colaboradores da Aurum palestras internas, a fim de dar ciência sobre:

- As políticas adotadas pela Aurum;
- A regulamentação vigente e aplicável aos negócios da Aurum; e
- Eventuais problemas ocorridos, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela Aurum.

Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do colaborador em lista de presença. Não sendo possível a participação do sócio ou colaborador, sua ausência deverá ser justificada ao Diretor de Compliance da Aurum, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela Aurum, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da Aurum, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Com relação aos procedimentos de controle e de prevenção à lavagem de dinheiro, a Aurum tem por princípio capacitar seus integrantes a observá-los. Adicionalmente, é esperado que sócios e colaboradores das áreas de relações com investidores, *back office*, mesa de operações, risco e compliance tenham um embasamento sério sobre a identificação de operações para crimes de lavagem de dinheiro.

O treinamento será realizado a cada 12 (doze) meses, e obrigatório a todos os colaboradores. Quando do ingresso de um novo colaborador, a Diretora aplicará o devido treinamento de forma individual para o novo colaborador. A Diretora poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os colaboradores constantemente atualizados em relação às Políticas.

O treinamento para capacitação de todos os colaboradores com relação às regras de prevenção à lavagem de dinheiro será realizado conjuntamente com o treinamento interno aqui referido. Os procedimentos de combate e prevenção à lavagem de dinheiro serão supervisionados pela Diretoria de Compliance, o qual terá livre acesso aos dados cadastrais dos clientes e colaboradores e às operações por estes realizadas.

ANEXO I
TERMO DE COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, declaro para os devidos fins que:

1. Recebi, li e compreendi os seguintes manuais e políticas internas da Aurum:
a. Política de Compliance e Controles Internos;
b. Código de Ética e Padrões de Conduta Profissional;
c. Política de Investimentos Pessoais;
d. Política de Prevenção à Lavagem de Dinheiro, ao Financiamento ao Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa e de Cadastro;
e. Política de Combate ao Suborno e Corrupção
f. Política de Seleção e Alocação de Ativos
g. Políticas Operacionais;
h. Política de Gestão de Riscos; e
i. Manual de Análise do Perfil do Investidor

2. Estou ciente de que as políticas e manuais acima passam a fazer parte dos meus deveres como colaborador da Aurum, incorporando-se às demais regras de conduta adotadas pela Aurum.

3. Comprometo-me, ainda, a informar imediatamente a Aurum qualquer fato que eu venha a ter conhecimento que possa gerar algum risco para a Aurum, incluindo, mas não se limitando, acerca de violações ou possíveis violações das políticas e manuais acima.

4. A partir desta data, a não observância de qualquer política interna poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis , ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos da Consolidação das Leis de Trabalho, ou desligamento ou exclusão por justa causa, conforme minha função à época do fato, inclusive eventual obrigação de indenizar a Aurum e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.

5. Entendo que as regras estabelecidas nas políticas internas da Aurum apenas servem de complemento e esclarecem como lidar com determinadas situações relacionadas à minha atividade profissional e, portanto, não invalidam nenhuma disposição contratual de trabalho e/ou societária.

6. Esclareci todas as minhas dúvidas relacionadas aos princípios e normas estabelecidos pela Aurum em seus manuais e políticas internas, de modo que as

compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento e de reciclagem a ser conduzido pela Aurum.

7. Tenho ciência de que a Aurum poderá monitorar toda e qualquer troca, interna ou externa, de meus e-mails, bem como meus acessos a sites e arquivos eletrônicos.

8. Declaro ciência e de acordo que são consideradas informações confidenciais ("Informações Confidenciais", ou, isoladamente "Informação Confidencial"), 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 Aurum, seus sócios e clientes, incluindo:

a) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais, incluindo, mas não se limitando a saldos, extratos e posições de clientes que a Aurum presta consultoria;

c) Operações estruturadas, demais operações e seus respectivos valores analisadas;

d) Relatórios, estudos, opiniões e apresentações internas sobre ativos financeiros exceto quando não o forem disponibilizados ao público em geral;

e) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

f) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Aurum e a seus sócios ou clientes;

g) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes;

h) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

i) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Aurum ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral; e

j) Quaisquer informações protegidas por acordos de confidencialidade firmados pela Aurum, bem como informações sigilosas de propriedade e/ou posse da Aurum, contrapartes e clientes, sejam de natureza comercial, jurídica, contábil, financeira, técnica, operacional ou de tecnologia, dados, planilhas, relatórios, respectivos clientes, potenciais clientes, lista de clientes, parceiros, potenciais parceiros, potenciais fornecedores, prestadores de serviços e potenciais prestadores de serviços, modelo de negócios, finanças, métodos contábeis, métodos gerenciais, estrutura de preços e custos, códigos-fonte, patentes, segredos comerciais, direitos autorais, logomarcas, apresentações, know-how, softwares, planejamento estratégico, informações pessoais ou de pessoas, fluxo de caixa e estratégias em geral.

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

10. O Colaborador 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 Aurum, se comprometendo, ainda a não utilizar, praticar ou divulgar informações privilegiadas, "Insider Trading" e "Front Running", seja atuando em benefício próprio, da Aurum ou de terceiros.

11. A não observância da confidencialidade e do sigilo, durante e mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal, além de esferas administrativas competentes.

12. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Aurum e terceiros, ficando deste já o Colaborador obrigado a indenizar a Aurum, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

13. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando devida sanção e possibilidade de desligamento/demissão por justa causa.

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

15. O Colaborador reconhece e toma ciência que:
a) 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, consultoria e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Aurum são e permanecerão sendo propriedade exclusiva da Aurum 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 Aurum, devendo todos os documentos permanecer em poder e sob a custódia da Aurum, salvo se em virtude de interesses da Aurum for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Aurum;

b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador motivado por qualquer das partes, ou seja, pela Aurum ou pelo Colaborador, ele deverá restituir imediatamente à Aurum todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e
c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e consultoria de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Aurum, 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.

16. Ocorrendo a hipótese do Colaborador 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 Colaborador deverá notificar imediatamente a Aurum, permitindo que a Aurum procure a medida judicial cabível para atender ou evitar a revelação.

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

16.2 A obrigação de notificar a Aurum subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

17. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do colaborador com a Aurum, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

18. A transgressão a qualquer das regras descritas neste Termo será considerada infração contratual, sujeitando o colaborador às sanções que lhe forem atribuídas pela Aurum.

_____

[COLABORADOR]