MANUAL DE COMPLIANCE

FULWOOD CAPITAL PARTNERS GESTÃO DE RECURSOS LTDA.

Março de 2026

ÍNDICE

1. INTRODUÇÃO

O presente Manual de Compliance ("Manual") visa assegurar, por meio de um controle interno adequado, o cumprimento permanente das regras, políticas e regulamentos atuais relacionados aos diferentes tipos de investimentos e à atividade de gestão de carteiras de valores mobiliários da **Fulwood Capital Partners Gestão de Recursos Ltda.** ("Fulwood Gestão") no exercício de suas atividades de gestão de recursos de terceiros, de acordo com a Resolução CVM nº 21, de 21 de fevereiro de 2021, conforme alterada ("Resolução CVM 21").

Todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética da Fulwood Gestão.

2. PROTEÇÃO DAS INFORMAÇÕES DE PROPRIEDADE EXCLUSIVA DA EMPRESA E DO INVESTIDOR

2.1. Procedimentos para a Divulgação Adequada de Informações

À luz das disposições de sigilo estabelecidas no Código de Ética, salvo se adequado no contexto de suas responsabilidades profissionais, um Colaborador Fulwood não poderá revelar a qualquer pessoa não associada à Fulwood Gestão (exceto: (i) àqueles envolvidos em uma operação ou com direito às informações em nome de um investidor; (ii) àqueles que prestem serviços jurídicos, contábeis, administrativos ou outros serviços ao respectivo fundo ou correntista; (iii) conforme exigido por lei; ou (iv) especificamente solicitado por tal investidor) qualquer informação relativa aos investidores, incluindo dados pessoais fornecidos à Fulwood Gestão por qualquer investidor; listas e arquivos de investidores ou outras informações do investidor; registros comerciais da Fulwood Gestão, informações de empregados, informações financeiras, software, licenças, contratos, arquivos de computador e planos de negócios; modelos, pesquisa de propriedade exclusiva, direitos autorais ou outros materiais pagos por um fundo ou pela Fulwood Gestão; e as análises e outros dados ou informações de propriedade exclusiva da Fulwood Gestão. Todas essas informações, sejam ou não materiais, são estritamente confidenciais e não podem ser divulgadas. Os Colaboradores Fulwood também não violarão as disposições de qualquer acordo de confidencialidade do qual a Fulwood Gestão ou o Colaborador Fulwood seja parte.

Os Colaboradores Fulwood não poderão divulgar informações relativas a recomendações ou possíveis operações que ainda não estejam assinadas ou que estejam sendo consideradas, exceto (i) conforme seja necessário; ou (ii) conforme exigido por lei (nesse caso, mediante notificação ao Diretor de *Compliance*, que deverá ser encaminhada por e-mail); e (v) após a informação estar de outra forma disponível ao público.

A Fulwood Gestão possui como dever primordial a lealdade a todo e qualquer investidor. Esse dever inclui a não apropriação indevidamente de informações e/ou estratégias desenvolvidas para uso na administração do capital da Fulwood Gestão com o objetivo de utilizá-las em negociações pessoais (ou negociações para outras contas) de tais Colaboradores Fulwood. De maneira geral, as políticas de negociações pessoais da Fulwood Gestão presentes no referido Código de Ética, bem como na Política de Compra e Venda de Valores Mobiliários da Fulwood Gestão devem evitar tal apropriação indevida, mas caso qualquer Colaborador Fulwood acredite estar em posição de lucrar com o uso de informações específicas que recebeu ou que foram geradas por conta da gestão dos investimentos da Fulwood Gestão, tal Colaborador Fulwood não deverá executar a operação em questão. Assim, indo ao encontro com as políticas internas da Fulwood Gestão.

3. TRATAMENTO DE DADOS

3.1. Titularidade de Dados

Com exceção do material claramente de propriedade de terceiros, tais como seus dados pessoais confidenciais, a Fulwood Gestão é a legítima titular de todas as informações comerciais armazenadas ou transmitidas através de seus sistemas. A menos que a Fulwood Gestão tenha celebrado um acordo específico por escrito, todas as informações comerciais desenvolvidas enquanto um Colaborador Fulwood estiver empregado pela Fulwood Gestão são de propriedade da Fulwood Gestão.

Os Colaboradores Fulwood, fornecedores e quaisquer outros terceiros não poderão copiar os softwares e/ou arquivos fornecidos pela Fulwood Gestão para qualquer meio de armazenamento, transferir tal software e/ou arquivo para outro computador ou divulgar tal software e/ou arquivo a terceiros externos sem permissão prévia do Diretor de *Compliance*.

4. CONTROLE DE ACESSO À INFORMAÇÃO

A Fulwood Gestão utiliza alguns mecanismos para garantir o controle de acesso a todas as suas informações e base de dados, conforme a seguir:

Senha para acesso

Todos os computadores e dispositivos que acessem o e-mail e/ou dados da Fulwood Gestão devem ter uma senha definida para todas as contas de usuário, incluindo de qualquer Colaborador Fulwood, e devem ser configurados para bloquear automaticamente a tela quando deixados sem supervisão após um determinado período. A Fulwood Gestão poderá, a seu critério, limitar a capacidade de um empregado ou de um destinatário de imprimir, encaminhar ou salvar um documento.

Criptografia

A Fulwood Gestão poderá utilizar software de criptografia que permita aos Colaboradores Fulwood garantir a segurança dos dados da Fulwood Gestão através do uso de e-mail e outros métodos de transmissão.

Acesso Remoto e Dispositivo Móveis

Todas os Colaboradores Fulwood podem acessar a rede da Fulwood Gestão de forma remota. A Fulwood Gestão reserva o direito de conduzir inspeções surpresa dos usuários com privilégios de acesso remoto visando à proteção e segurança dos dados e informações da Fulwood Gestão.

O acesso remoto, pela sua natureza, tem um nível de risco inerentemente mais elevado. O acesso remoto aos sistemas Fulwood Gestão está disponível de diversas maneiras, dependendo do dispositivo que o Colaborador Fulwood está utilizando e das necessidades do seu trabalho. Isso inclui aplicativos da web, serviços de área de trabalho remota e VPN.

A Intranet da Fulwood Gestão está disponível apenas para Colaboradores Fulwood e determinados parceiros de extranet de acordo com a necessidade.

Outros aplicativos baseados na web estão disponíveis para funcionários e parceiros de extranet conforme a necessidade.

O acesso dos serviços de área de trabalho remota a aplicativos e serviços está disponível para Colaboradores Fulwood e parceiros de extranet com base na necessidade.

O acesso VPN completo está disponível apenas para Colaboradores Fulwood que usam um computador gerenciado pela Fulwood Gestão, e o computador deve estar executando aplicativos antimalware e firewall aprovados atualmente.

A VPN limitada está disponível para não funcionários onde suas responsabilidades exigem tal acesso.

Solicitações de acesso remoto: O acesso remoto é permitido aos Colaboradores Fulwood desde que sejam utilizados os métodos de conexão e os dispositivos necessários. Quando o acesso remoto for necessário para qualquer não funcionário, esse acesso só poderá ser fornecido após aprovação da Diretoria de *Compliance*.

Dispositivos de acesso remoto aprovados: Equipamentos fornecidos pela Fulwood podem ser usados para estabelecer conexões de acesso remoto. Além disso, equipamentos de propriedade do usuário que tenham sido autorizados pelo time de tecnologia da informação da Fulwood Gestão ("TI") para uma finalidade comercial específica poderão ser usados; caso contrário, os equipamentos de propriedade do usuário não poderão ser usados para conectividade VPN; entretanto, esses dispositivos podem se conectar por meio de outros métodos mencionados anteriormente. Computadores pessoais domésticos não

gerenciados pelo time de TI e, portanto, não podem ser garantidos que estejam protegidos pelos padrões de segurança corporativa da Fulwood. Eles são considerados dispositivos inseguros. Os dados da Fulwood não devem ser armazenados em nenhum dispositivo inseguro.

Acesso remoto à rede local: os dispositivos que se conectam remotamente à rede local devem cumprir o seguinte:

- Todos os computadores conectados a redes internas através de tecnologias de acesso remoto devem ter um sistema operacional atualizado e proteção de *endpoint* aprovada e atualizada;

- A autenticação de dois fatores é necessária antes que o acesso à rede possa ser concedido.

Controle remoto de dispositivos: somente tecnologia e software de controle remoto de dispositivos aprovados pela TI podem ser usados para controlar remotamente um servidor, computador, smartphone, aplicativo, etc., e somente sob as seguintes condições:

- O controle remoto só será usado como uma ferramenta para conexão com o próprio computador de trabalho, para cumprir as próprias responsabilidades profissionais.

- O procedimento para o pessoal de TI acessar/controlar remotamente a estação de trabalho de outra pessoa é entrar em contato com o usuário da estação de trabalho por telefone para notificá-lo sobre o acesso necessário.

- O uso de *software* de controle remoto para acessar o computador de outra pessoa é limitado ao pessoal autorizado de TI e aos prestadores de serviços terceirizados autorizados.

Acesso Remoto para Diagnóstico/Manutenção: todas as conexões de acesso remoto para diagnóstico e manutenção de equipamentos devem ser configuradas de forma a garantir a conformidade com o acesso remoto.

O acesso às redes por meio de mecanismos de comunicação sem fio não seguros é estritamente proibido. Os Colaboradores Fulwood só podem conduzir negócios da Fulwood Gestão e conectar-se à rede sem fio dos Colaboradores Fulwood usando dispositivos seguros e autorizados pela Fulwood Gestão. Dispositivos externos, como os usados pelos visitantes, só podem se conectar à rede sem fio do Convidado.

Armazenamento móvel:

Devido à natureza portátil das mídias de computador, como CDs, DVDs, discos rígidos removíveis, unidades flash USB, etc., esses dispositivos são considerados inseguros, a menos que sejam criptografados. Para dispositivos utilizados por funcionários que possam ter acesso a informações privilegiadas, o uso de dispositivos de armazenamento USB pode ser desativado por meio da Política da Fulwood Gestão.

Programas Antivírus

No âmbito deste Manual, a Fulwood Gestão atualizará os sistemas operacionais e software em sua rede quando necessário; tais atualizações ajudarão a reduzir as vulnerabilidades da rede, uma vez que as atualizações frequentemente abordam ameaças conhecidas ou antecipadas.

A Fulwood Gestão monitorará regularmente eventos e conexões através do *firewall* da Fulwood Gestão para detectar quaisquer violações, ataques ou acesso a informações sensíveis. A Fulwood Gestão garantirá que softwares antivírus sejam instalados em todos os computadores, que o acesso ao servidor seja definido e periodicamente auditado e que privilégios de administrador sejam implementados.

Equipamentos Extraviados

Caso um computador laptop ou dispositivo móvel seja extraviado ou roubado, ou esteja fora do controle de um empregado por mais de 24 (vinte e quatro) horas, o empregado deverá notificar o setor TI, que tomará as devidas precauções para desativar as informações para o laptop ou dispositivo móvel. Além disso, todos os computadores, laptops, *tablets* e telefones celulares dos empregados são criptografados, tornando os dados ilegíveis em caso de perda ou roubo.

Acesso à internet e redes sem fio

O acesso à internet é fornecido para a Fulwood Gestão e é considerado um recurso para a gestora. O acesso à Internet fornecido pela Fulwood Gestão não deve ser usado para entretenimento, tão somente como ferramenta de pesquisa e trabalho.

Os nomes e senhas das redes sem fio estão sujeitos a alterações por razões de segurança a qualquer momento, com pouca ou nenhuma notificação. A Fulwood Gestão implementou pontos de acesso sem fio para conceder acesso exclusivamente aos recursos da internet. Os dispositivos e usuários nesta rede são separados por um *firewall* dos recursos internos da rede. Os usuários finais estão proibidos de instalar pontos de acesso sem fio para sua própria conveniência. Os pontos de acesso sem fio devem ser protegidos.

Nenhum ponto de acesso sem fio pode ser conectado à rede "Fulwood (Z:)" sem aprovação expressa por escrito da TI. Qualquer ponto de acesso sem fio aprovado deve ser

configurado de acordo com as especificações atuais de configuração de TI da Fulwood. Qualquer ponto de acesso sem fio que não esteja registrado junto à TI ou não esteja configurado corretamente será desconectado imediatamente da rede "Fulwood (Z:)".

Detalhes adicionais da rede sem fio:

- O acesso sem fio é separado em duas redes distintas o (i) "FULWOOD" e (ii) "FULWOOD_CORP", cujo acesso é controlado por WPA2 e protegido por senha.

5. SEGURANÇA CIBERNÉTICA (CIBERSEGURANÇA)

Um incidente de segurança cibernética é qualquer evento, violação de controle ou mau funcionamento de software que possa representar uma ameaça à confidencialidade, integridade ou disponibilidade de sistemas, aplicativos ou informações de suporte. Todos os incidentes de segurança cibernética devem ser imediatamente relatados à TI. A equipe de TI deve relatar imediatamente cada incidente à Equipe de *Compliance*. A notificação inicial do incidente pode ser fornecida pessoalmente, por e-mail ou por telefone; no entanto, a TI deve documentar imediatamente o incidente em um tíquete de central de serviços. O gerenciamento de TI avaliará o incidente e determinará o curso de ação apropriado.

Avaliação de ameaças e vulnerabilidades

As empresas usam uma variedade de informações em seu processo de avaliação de risco. No que diz respeito às ameaças, estas informações incluem incidentes de segurança cibernética anteriores, quer na empresa, quer observados na indústria, informações sobre ameaças identificadas por outras organizações ou através de organizações de segurança, como o Centro de Análise e Partilha de Informações de Serviços Financeiros (FS-ISAC). Essas ameaças podem incluir ameaças internas – por exemplo, ameaças de funcionários – ou ameaças externas, como *hacktivistas* ou grupos do crime organizado. Outro componente importante do processo de avaliação de riscos é a análise de vulnerabilidades – o processo de identificação, quantificação e priorização de vulnerabilidades potenciais dentro de um sistema. A sofisticação da análise de vulnerabilidade varia entre as empresas. Uma abordagem comumente usada é o *Common Vulnerability Scoring System* ("CVSS") para avaliar vulnerabilidades em aplicativos. CVSS é um padrão aberto do setor para avaliar a gravidade das vulnerabilidades e priorizar sua correção. Os resultados destas revisões são utilizados como contributos para o programa de avaliação de risco da empresa e orientariam as classificações de risco de vários ativos críticos.

Alertas de dispositivos de segurança de rede

Conforme apropriado, alertas de dispositivos de segurança de rede, incluindo, entre outros, firewalls, detecção de intrusão ou tecnologias de prevenção, devem ser coletados em conjunto com qualquer investigação de um incidente de segurança da informação.

Revisão do Processo de Resposta a Incidentes Cibernéticos

O plano de resposta a incidentes cibernéticos é continuamente revisado e atualizado, pelo menos anualmente, para garantir que o plano seja consistente e viável com quaisquer mudanças nas reestruturações organizacionais, níveis de pessoal, tendências do setor e avaliações de risco. Um exercício de "*Lições Aprendidas*" é realizado no final de uma resposta real a um incidente, e exercícios de mesa periódicos garantem que cada departamento de partes interessadas especializado no assunto esteja ciente de suas responsabilidades e capacidades.

Escalação de Incidentes

- Qualquer impacto material ou potencial impacto material deve ser encaminhado imediatamente à Equipe de *Compliance*.
- A Equipe de Compliance avaliará e classificará a materialidade do impacto ou impacto potencial;
- Todos os incidentes serão remediados com uma prioridade adequada ao impacto e em relação a quaisquer outros incidentes abertos.

Requisitos de informações para relatórios de incidentes

Um relatório de incidente deve incluir:

- Detalhes de contato do notificador de incidentes (área funcional, nome, telefone);
- Data e hora do incidente;
- Data e hora da resolução;
- Tipo de incidente;
- Tipo de dados envolvidos;
- Causa raiz;
- Classificação de gravidade (alta, média, baixa);
- Descrição do incidente (incluir a fonte do incidente, se conhecida, mas não deve incluir a identificação de qualquer indivíduo específico);
- Impacto do incidente (real ou potencial);
- Resolução de incidente (ação de resolução e prevenção de recorrência);
- Informações técnicas (conforme listadas no formulário);

- Conforme apropriado, quaisquer alterações necessárias na infraestrutura, software ou controles para evitar um futuro incidente semelhante.

Tipos de Incidentes

A descrição dos tipos de incidentes inclui, mas não está limitada ao seguinte:

- Violação da política;
- Fraqueza de segurança;
- Comprometimento da conta;
- Vulnerabilidade comportamental;
- Corrupção de dados/informações;
- Negação de serviço;
- Divulgação (uso indevido) de dados/informações;
- Comprometimento da rede;
- Comprometimento de senha;
- Segurança física;
- Sondas (não autorizadas);
- Violações de políticas;
- Roubo (de dados);
- Roubo (de coisa física);
- Acesso e/ou uso não autorizado;
- Vírus;
- Violação de segurança em fornecedores terceirizados críticos.

Objetivo e Escopo

A intenção do Plano de Resposta a Incidentes Cibernéticos é fornecer um processo estabelecido sobre como responder a um incidente de segurança da informação. Este plano não é uma lista de verificação passo a passo exaustiva, mas uma visão geral das fases e da ordem de ações de alto nível. Este plano entende que cada departamento especializado no assunto mantém seu próprio plano de resposta a incidentes, sejam eles relacionados à

segurança da informação ou não, e, portanto, depende de seus respectivos planos de resposta para lidar com suas atividades de resposta específicas. O plano a seguir foi concebido principalmente a partir de uma perspectiva de TI, com a intenção não de ser um guia abrangente para todas as atividades de resposta a incidentes cibernéticos, mas de ser o guia geral e o catalisador para ativar os planos de resposta diferentes e específicos de cada especialista no assunto e parte interessada. Este plano de resposta a incidentes aborda todos os incidentes relacionados à segurança cibernética, sejam eles ocorridos no ambiente corporativo da Fulwood ou em um ativo/edifício individual da Fulwood.

Fases de Resposta a Incidentes Cibernéticos

Embora os detalhes da resposta a cada incidente variem muito, o esboço geral pode ser visto nas fases seguintes.

1. Identificação;

2. Remediação;

3. Acompanhamento e Lições Aprendidas;

4. Atualizar o plano de resposta a incidentes cibernéticos (inclui informar a todos sobre as atualizações);

5. Atualizações periódicas do plano, testes, exercícios de mesa, etc.

Visão geral da resposta a incidentes cibernéticos

A seguir está uma visão geral de alto nível do processo de resposta a incidentes cibernéticos. Cada etapa pode ter muitas subetapas, embora essas subetapas não sejam descritas neste documento.

1. Notifique a gestão de TI assim que um problema cibernético for identificado. O método específico para notificar o gerenciamento de TI não é tão importante quanto a notificação ocorrer assim que um incidente potencial for identificado.

2. A gestão de TI avaliará se o problema é de fato um incidente e se requer escalonamento.

3. A TI comunica periodicamente o status aos usuários afetados e ao gerenciamento de tecnologia da informação, bem como recomenda soluções provisórias para minimizar a interrupção dos negócios.

4. Quando apropriado, um relatório de resposta a incidentes cibernéticos será emitido para a gestão de TI, documentando o evento e as ações de remediação.

5. A gestão de TI avalia se deve envolver o seu parceiro externo de resposta a incidentes cibernéticos, tendo em conta, entre muitos fatores, o âmbito do incidente, a capacidade dos recursos internos para conter e remediar o incidente, o tempo esperado necessário para remediar o incidente, o risco de interrupção dos negócios, o risco de dados comprometidos, etc.

6. Se apropriado, envolver o parceiro externo pré-estabelecido de resposta a incidentes cibernéticos da Fulwood.

7. Siga as instruções do parceiro de resposta a incidentes. Remediação completa do incidente.

8. Se for descoberto qualquer uso ou divulgação não autorizada de informações pessoais, a Equipe de *Compliance* determinará as próximas etapas e os requisitos de relatório.

9. Cada departamento especializado no assunto se reúne para discutir as lições aprendidas e quaisquer atualizações em seus respectivos processos.

6. CONFIDENCIALIDADE

Os Colaboradores Fulwood tratarão como confidencial e não revelarão ou divulgarão em circunstância alguma, independentemente da forma em que tais informações sejam divulgadas, comunicadas ou mantidas, qualquer documento ou informação relacionada à Fulwood Gestão e os fundos geridos por ela, seus investimentos potenciais e efetivos, seus investidores, clientes e prestadores de serviços, incluindo, mas não se limitando a, negociações, métodos, modelos, senhas, pesquisas, arquivos de computador, informações e registros financeiros, programas de software de computador, acordos e/ou contratos, políticas, práticas, conceitos e estratégias de marketing e/ou de criação e métodos de operação, políticas internas, políticas e procedimentos de preços, estimativas de custos, listas de empregados, projeções financeiras ou comerciais, assim como qualquer informação sobre ou recebida de clientes e outras empresas com as quais a Fulwood Gestão mantenha um relacionamento comercial.

Além disso, no curso de seus negócios, a Fulwood Gestão celebra acordos de não-divulgação e acordos de confidencialidade com terceiros relacionados a potenciais oportunidades de investimento. A Fulwood Gestão espera que todos os Colaboradores Fulwood obedeçam às restrições impostas por esses acordos, incluindo não compartilhar informações de ou sobre essas empresas com qualquer um que não seja funcionário da Fulwood Gestão.

Não obstante o acima exposto, sempre que uma informação relevante não pública for recebida, os profissionais de investimento da Fulwood Gestão serão responsáveis por informar ao Diretor de *Compliance*, para que este possa dar seguimento a todos os procedimentos aplicáveis, bem como dar as devidas recomendações.

Por fim, cada Colaborador Fulwood é responsável por manter a segurança adequada dos registros da Fulwood Gestão e de todos os materiais e informações que não se destinam ao conhecimento público. De forma exemplificativa, as seguintes precauções devem ser tomadas por cada Colaborador Fulwood:

- Antes de sair da sede da Fulwood Gestão, cada Colaborador Fulwood deve verificar se existem documentos confidenciais nas áreas comuns de trabalho;

- Os escritórios individuais devem ser trancados sempre que possível;

- Todas as cópias físicas de contratos, cartas de compromisso, documentos de incorporação, documentos de venda, dentre outros, devem ser arquivados em locais com senha assim que razoavelmente possível;

- Todos os meios eletrônicos devem ser protegidos adequadamente (por senhas e práticas de gerenciamento de informações) e não devem ser copiados ou compartilhados de maneira inadequada fora ou dentro da Fulwood Gestão;

- Cada Colaborador Fulwood deve ter um cuidado extra com propostas, licitações, relatórios de gestão, relatórios de locação, relatórios de custos, dentre outros. Cópias físicas desses documentos devem ser mantidas em arquivos trancados sempre que possível.

- Qualquer informação potencialmente confidencial não deve ser discutida fora do escritório (ou seja, elevadores, reuniões públicas). Os Colaboradores Fulwood devem exercer discrição e cautela ao discutir informações confidenciais que possam afetar materialmente uma transação comercial pendente ou resultar em divulgação imprópria de informações materiais não públicas.

- Registros financeiros, incluindo demonstrações financeiras auditadas e não auditadas, estatísticas financeiras, qualquer informação sobre funcionários, manuais, declarações de impostos, diretrizes e manuais operacionais, materiais de treinamento, relatórios de avaliação de propriedade e todos os outros materiais de natureza confidencial, dentre outros, não devem ser distribuídos para qualquer pessoa não autorizada (dentro ou fora da empresa).

- Todos os materiais produzidos ou recebidos por um Colaborador Fulwood e todos os itens contidos nos arquivos do Colaborador Fulwood são propriedade da Fulwood Gestão e não devem ser removidos das instalações da Fulwood Gestão ou usados para fins diferentes dos negócios da Fulwood Gestão.

7. TREINAMENTO

Como parte de seu programa de Controles Internos, a Fulwood Gestão dará treinamento sobre este Manual para todas as Colaboradores Fulwood e, se necessário, para afiliados e

fornecedores. O treinamento pode incluir, entre outros tópicos, instrução sobre a criação de senhas fortes, detecção de e-mails de *phishing*, dispositivos aprovados, sincronização de dispositivos pessoais e redução da exposição a e-mails. O treinamento ocorrerá periodicamente e sua frequência dependerá de uma série de fatores incluindo, mas não se limitando à evolução das ameaças à segurança. O treinamento pode se dar na forma de reuniões em toda a empresa, distribuição de materiais escritos ou orientação fornecida por e-mail. O Diretor de *Compliance* será responsável por manter um registro de quaisquer orientações ou materiais escritos fornecidos durante tal treinamento.

Os treinamentos são realizados sempre que o Diretor de *Compliance* achar necessário e no momento da integração de um novo Colaborador Fulwood, conforme exposto a seguir:

Treinamento de Integração

Quando da contratação de um Colaborador Fulwood e, antes do início efetivo de suas atividades, ele participará de um processo de integração e treinamento onde adquirirá conhecimento sobre as atividades da empresa, regras, políticas e códigos internos, assim como informações sobre as principais leis e regulamentos que regem as atividades da Fulwood Gestão.

Treinamento contínuo

A Fulwood Gestão adota um programa anual de reciclagem dos Colabores Fulwood, a fim de garantir que eles estejam sempre atualizados sobre os termos e responsabilidades aqui descritos, estando todos obrigados a participar de tais programas de reciclagem.

Além disso, no caso de qualquer mudança nas políticas empregadas pela Fulwood Gestão e/ou da regulamentação aplicável às atividades desenvolvidas pela Fulwood Gestão, a Fulwood Gestão poderá conduzir um treinamento a fim de apresentar as mudanças e novos pontos abordados por tal política.

Finalmente, deve-se observar que o processo de treinamento inicial e o programa de reciclagem contínua são desenvolvidos e controlados pelo Diretor de Compliance e exigem o compromisso total dos empregados com seu atendimento e dedicação.

8. SEGURANÇA DA INFORMAÇÃO

8.1. Privacidade dos Empregados

Os Colaboradores Fulwood não devem ter qualquer expectativa de privacidade ao utilizar os sistemas de informação na Fulwood Gestão. Para gerenciar sistemas e reforçar a segurança, a Fulwood Gestão pode registrar, revisar e utilizar qualquer informação armazenada ou que circule através de seus sistemas. A Fulwood Gestão pode capturar atividades dos usuários como tráfego de e-mail, números de telefone discados e sites visitados. Além disso, a administração da Fulwood Gestão reserva-se o direito de monitorar,

inspecionar ou remover de seus sistemas de informação qualquer material que considere ofensivo ou potencialmente ilegal. Esse exame pode ocorrer com ou sem o consentimento, presença ou conhecimento dos Colaboradores Fulwood envolvidas. Os sistemas de informação sujeitos a tal exame incluem, mas não estão limitados, a sistemas de correio eletrônico, qualquer dispositivo controlado pela Fulwood Gestão, arquivos de correio de voz, arquivos de *spool* de impressora, saída de fax, gavetas de mesa e áreas de armazenamento.

8.2. Uso Pessoal de Sistemas e Armazenamento de Dados Pessoais

Os sistemas de informação da Fulwood Gestão são destinados à utilização somente para fins comerciais. Os arquivos pessoais de um Colaborador Fulwood, tais como documentos, fotos, vídeos ou música, não devem ser armazenados no disco compartilhado da Fulwood Gestão. O uso pessoal acidental é permitido se não for um risco, não consumir mais do que uma quantidade trivial de recursos que poderiam ser usados para fins comerciais, não interferir na produtividade do usuário e não impedir qualquer atividade comercial. É proibido o uso dos sistemas de informação da Fulwood Gestão para correspondência em cadeia, solicitações de caridade, material de campanha política, trabalho religioso, transmissão de material questionável, ou qualquer outro uso não comercial. Software pessoal não deve ser instalado nos sistemas de informação da Fulwood Gestão sem a aprovação expressa do Diretor de Compliance. A Fulwood Gestão não é responsável por quaisquer dados pessoais armazenados nos computadores ou servidores da empresa e poderá apagar esses dados sem aviso prévio. Além disso, a Fulwood Gestão não investirá recursos da empresa na recuperação de dados pessoais no caso de perda dos mesmos.

9. PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

O objetivo do Plano de Contingência e Continuidade de Negócios visa estabelecer as medidas a serem tomadas para evitar um impacto negativo na condução das atividades desenvolvidas pela Fulwood Gestão, como, por exemplo, crises econômicas nacionais e/ou mundiais, pandemias, falhas operacionais e/ou desastres naturais.

<u>Estratégia de Continuidade de Negócios da Fulwood</u>

- Escritório Corporativo e Equipe

A sede corporativa e a equipe da Fulwood Gestão é localizado em São Paulo, no Brasil. No caso de um desastre que torne o escritório de São Paulo inoperante, a equipe trabalhará remotamente em locais dispersos, como residências particulares, hotéis, escritórios de terceiros ou outros locais.

- Departamentos de Missão Crítica

A Fulwood reconhece que um desastre que destruísse seu escritório ou instalações de informática representaria um risco operacional significativo. Para mitigar esse

risco, a Fulwood possui políticas e procedimentos que constituem um programa corporativo de continuidade de negócios.

Preparação para o Cenário de Negócios

- Locais de escritórios

Para garantir que a Fulwood esteja pronta para responder de maneira coordenada a desastres naturais e emergências, recursos estão disponíveis para seu escritório para a criação de um plano de contingência e resposta de emergência personalizado e específico. Se a Fulwood perder a capacidade de realizar negócios em seu escritório, as funções serão realocadas para um local alternativo (por exemplo, outro local, casa, hotel, local de terceiros) em uma área não afetada.

- Centro de dados remoto

Se a Fulwood perder a capacidade de realizar negócios em seu local principal hospedado na nuvem, a TI e seu parceiro técnico farão o failover para seu local de recuperação de desastres.

- Evento Pandêmico

A Fulwood Gestão tem planos para continuar os negócios durante um evento de pandemia. É um plano de ação multinível baseado nas orientações da Organização Mundial da Saúde (OMS).

10. CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

O objetivo deste dispositivo é estabelecer critérios qualitativos mínimos e orientar o processo de seleção, contratação e monitoramento de indivíduos e entidades que possam ter interesse em iniciar e manter um relacionamento comercial com a Fulwood Gestão.

Este é um procedimento real de *Know Your Partner* - KYP, focado no conhecimento do terceiro a ser contratado, nos procedimentos de integridade instituídos e observados pelas empresas que operam com a Fulwood Gestão.

Os critérios e processos aqui estabelecidos visam proporcionar o mínimo indispensável de segurança operacional e jurídica, evitando conflitos de interesse de forma a manter a Fulwood Gestão em conformidade com o Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros e outras normas e regras aplicáveis à matéria.

10.1. Análise de Mercado

- Sempre avaliar se esse prestador de serviços pode gerar qualquer potencial conflito de interesse com o gestor de recursos, administrador fiduciário ou cotista dos veículos de investimento administrados pela Fulwood Gestão;

- Se o valor cobrado é justo em relação ao serviço oferecido e ao valor de mercado;

- Se há benefícios recebidos pela Fulwood Gestão e seus empregados derivados de tal contratação, ou se os benefícios são direcionados ao fundo ou ao investidor.

10.2. Processo de Pré-Seleção

Durante o processo de contratação, os empregados devem obter informações qualitativas sobre o terceiro interessado em iniciar vínculos legítimos com a Fulwood Gestão, a fim de permitir um melhor julgamento durante a pré-seleção. As informações a serem obtidas devem incluir:

- A data de início das atividades;

- Qualificações dos principais sócios/executivos;

- Lista de clientes (passados e atuais) e objeto da contratação;

- Busca na rede mundial de computadores sobre notícias negativas sobre o terceiro; e

- Outras informações qualitativas que possam ser relevantes para melhor avaliar o terceiro.

O terceiro deverá estar legalmente constituído, gozar de boa reputação, ter capacidade econômica, financeira e técnica compatível com o objeto do contrato e com a assunção de responsabilidades contratuais.

Cópias do cartão de registro no Cadastro Nacional da Pessoa Jurídica (CNPJ) e documentos constitutivos e/ou corporativos relevantes devem ser solicitados ao terceiro. Se necessário, devem ser solicitadas cópias das demonstrações financeiras dos últimos 3 (três) anos e referências bancárias e técnicas do terceiro.

Além disso, os seguintes aspectos devem ser considerados durante o processo de pré-seleção:

- Estrutura da empresa;

- Boa reputação (no caso de uma pessoa jurídica, a reputação dos sócios e dos principais executivos também deve ser considerada);

- Nível de satisfação de outros clientes, passados e presentes;
- Estrutura para atender o objeto da contratação;
- Capacidade econômica e financeira;
- Código de Conduta e Ética, ou similar;
- Política Anticorrupção, ou similar;
- Política de Combate à Lavagem de Dinheiro, ou similar;
- Qualquer documento, procedimento e/ou formulário relacionado com a integridade e o cumprimento das regras; e
- Selo de Associado ou Aderente à ANBIMA, quando aplicável, ou, se não for o caso, as razões para não o obter.

O início das atividades dos empregados estará vinculado à formalização do contrato, e nenhum pagamento poderá ser feito antes da conclusão do contrato. Os acordos celebrados para formalização do contrato deverão ter os requisitos contidos no artigo 11 do Código ANBIMA de Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros.

Os empregados responsáveis pelo processo de seleção de fornecedores manterão registros atualizados dos fornecedores, eliminando aqueles sobre os quais haja qualquer dúvida relativa a má conduta, comportamento antiético, comportamento ilícito ou que possam ter uma má reputação no mercado.

10.3. Não Aplicabilidade do Processo de Pré-Seleção

A Fulwood Gestão poderá deixar de aplicar os procedimentos ora estabelecidos, a seu critério exclusivo, quando o terceiro não estiver relacionado ao negócio principal do gestor de recursos e tiver uma clara capacidade econômica, financeira e/ou técnica para satisfazer o objeto da contratação e para cumprir suas responsabilidades e arranjos contratuais.

10.4. Outras Disposições

Vale mencionar que, devido às regras estabelecidas na atual regulamentação e autorregulamentação, a Fulwood Gestão adotará medidas prévias de *due diligence* para a contratação e monitoramento de terceiros relacionados à tecnologia, sistemas e/ou infraestrutura de informação, visando à proteção de dados.

10.5. Seleção de Corretores

A Fulwood Gestão, com a prestação de serviços adequados que garantam a melhor execução das ordens para veículos de investimento e/ou carteiras administradas sob gestão, juntamente com a preservação dos interesses e, consequentemente, de seus investidores, adota um cuidadoso processo de seleção e contratação de corretores.

Esse processo é baseado na devida investigação de potenciais corretores-distribuidores de valores mobiliários para permitir que a Fulwood Gestão adquira um conhecimento profundo de potenciais prestadores de serviços.

Os corretores devem ser considerados como terceiros, para fins de aplicação do Processo de Pré-seleção, incluindo solicitando à corretora a certificação do Programa de Qualificação Operacional (PQO) da B3 e o questionário padrão de *due diligence* da Anbima.

10.6. Monitoramento

O monitoramento das atividades realizadas por terceiros para a Fulwood Gestão, assim como os próprios terceiros, é de responsabilidade da área que solicitou a contratação. O monitoramento deve ser contínuo durante a vigência da contratação, e o terceiro avaliado proporcionalmente ao serviço prestado, com ênfase em eventuais disparidades de tempo, qualidade e quantidade esperada.

Além disso, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a Fulwood Gestão, e os respectivos relatórios devem ser enviados para a Equipe de *Compliance*.

No caso de qualquer fato novo ou mudança significativa, é possível reavaliar a contratação de terceiros.

É importante notar que este monitoramento se baseia no princípio dos melhores esforços, já que a Fulwood Gestão e seus empregados não podem estar presentes no dia a dia de terceiros contratados a todo tempo.

10.7. Manutenção de Documentos

Todos os manuais, relatórios, atas e outros documentos relacionados a essa seleção de terceiros e à Política de Contratação de Terceiros serão mantidos em arquivos físicos ou armazenados digitalmente no escritório da Fulwood Gestão por um mínimo de cinco (05) anos.

11. VIOLAÇÃO E MEDIDAS DISCIPLINARES

A violação desta Política pode resultar em aplicação pelo Diretor de *Compliance* das sanções que julgar apropriadas, incluindo, entre outras coisas, uma carta de censura, suspensão ou rescisão do contrato de trabalho do infrator. A Fulwood Gestão se reserva o direito de notificar as autoridades competentes de aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade.

12. DISPOSIÇÕES GERAIS

Esta Política está disponível no website da Fulwood Gestão, de acordo com o Artigo 16, III da Resolução CVM 21.

13. VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado anualmente pela Fulwood Gestão e será alterado na medida em que houver a necessidade de atualizar seu conteúdo.

* * *