MANUAL DE COMPLIANCE

REAL WEALTH MULTI FAMILY OFFICE LTDA.

DOCUMENTO PÚBLICO

HISTÓRICO DE VERSÕES E ATUALIZAÇÕES

Versão	Data de publicação	Natureza	Responsável
02/2025	102025	Documento público	Diretor de Compliance e Comitê de Compliance

1. SUMÁRIO

2. OBJETIVO E APLICABILIDADE

Este Manual de Compliance ("Manual") apresenta as principais políticas, regras e procedimentos que orientam o desenvolvimento das atividades da **REAL WEALTH MULTI FAMILY OFFICE** ("Gestora"), além de fornecer uma descrição detalhada dos principais controles e procedimentos vigentes nesta data. Este documento se destina a todos os Colaboradores da Gestora, assim compreendidos todos os sócios, associados, funcionários, estagiários, temporários, trainees e terceiros alocados nas dependências da Gestora (em conjunto "Colaboradores "e individualmente "Colaborador").

O presente Manual tem por objetivo definir as diretrizes, procedimentos e controles adotados pela Real Investor para prevenir, identificar, detectar e corrigir quaisquer práticas que possam violar a regulamentação aplicável ao mercado de capitais.

Além de orientar a conduta dos Colaboradores e parceiros, este Manual reflete o compromisso da Gestora com a integridade, a transparência e a conformidade perante os órgãos reguladores e autorreguladores, promovendo uma cultura de controles internos eficazes e aderente às melhores práticas de governança.

Este Manual deve ser continuamente observado por todos os integrantes da organização, assegurando que os processos internos estejam sempre em conformidade com o ambiente regulatório vigente.

Este Manual aplica-se a todos os Colaboradores da Gestora.

2.1. BASE LEGAL

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

- Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21");
- Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM 50");
- Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175") e seus Anexos Normativos;

- Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("Anbima") de Ética ("Código Anbima de Ética");
- Código de Administração e Gestão de Recursos de Terceiros ("Código de AGRT");
- Regras e Procedimentos do Código de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III;
- Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, , de 11 de julho de 2022, conforme alterada ("Normas de Anticorrupção");
- Lei 9.613, de 03 de março de 1998, conforme alterada; e
- Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora.

3. INFORMAÇÕES REGULATÓRIAS

A Gestora é registrada junto à Comissão de Valores Mobiliários ("CVM") como administradora de carteiras de valores mobiliários, na categoria gestor de recursos, conforme ato declaratório nº 11.303 de 27 de setembro de 2010.

4. SUPERVISÃO DAS ÁREAS INTERNAS:

Área	**Nome**
Gestão	Diego Rodriguez
Operações	Marcelo Nobre Frasson
Risco	Elber Ogasavara
Compliance	Amanda Palmieri
PLD/FTP	Amanda Palmieri
DPO (Encarregado de Proteção de Dados)	Marcelo Nobre Frasson

5. REPRESENTAÇÃO LEGAL E ENDEREÇOS

A Gestora será representada por seus administradores, conforme previsto em seu Contrato Social. Além disso, compete exclusivamente a eles, ou às pessoas autorizadas por eles, a representação da Gestora perante a mídia, agentes públicos, do governo, reguladores e autorreguladores.

Nossa sede fica localizada na Cidade de São Paulo, Estado de São Paulo, na Rua Iguatemi, nº 192, 15º andar, sala 151, Edifício Iguatemi Offices Building, Itaim Bibi, CEP 01.451-010..

6. ESTRUTURA DE COMPLIANCE E RESPONSABILIDADES

A coordenação e supervisão das atividades previstas neste Manual é do Diretor de Compliance e PLD ("Diretor de Compliance"), assim designado nos termos do contrato social da Gestora.

Em conformidade com o disposto no normativo da CVM e em linha com os princípios da autorregulação da ANBIMA, o Diretor de Compliance exerce suas funções com autonomia plena e independência funcional, de modo a assegurar a sua isenção na identificação de irregularidades e reporte de situações de não conformidade.

É da competência do Diretor de Compliance:

- a orientação dos Colaboradores quanto à interpretação e aplicação deste Manual e das normas regulatórias vigentes;
- a supervisão e o monitoramento da aderência da instituição aos controles internos e à legislação aplicável; a promoção de treinamentos periódicos e ações de capacitação em compliance e integridade;
- a avaliação e o reporte em casos de descumprimento às instâncias competentes, em especial ao Comitê de Compliance;
- encaminhar aos órgãos de administração da Gestora, até o último dia útil do mês de abril de cada ano, relatório anual de compliance referente ao ano civil imediatamente anterior à data de entrega;
- elaborar relatório anual listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa – PLDFTP e de Cadastro da Gestora ("Política de PLDFTP"), devendo referido relatório permanecer disponível à CVM na sede da Gestora, sendo certo que este relatório de PLDFTP poderá constar no mesmo documento do relatório de compliance, mencionado acima;
- analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais;
- Assuntos de Certificação, tratados na Política de Certificação;

- a coordenação da gestão do canal de denúncias, assegurando o anonimato, sigilo e tratamento adequado das comunicações recebidas e, por fim, a guarda dos registros organizados das atividades de compliance e o reporte, quando aplicável, às autoridades reguladoras ou autorreguladoras. CIO / CEO e COO podendo haver membros convidados.

As atividades do Diretor de Compliance contarão com o suporte da equipe de compliance ("Equipe de Compliance"), que será responsável por apoiar o acompanhamento das regras estabelecidas neste Manual, prestar orientação aos Colaboradores e contribuir para a prevenção e identificação de eventuais condutas em desconformidade com suas disposições.

7. DA GOVERNANÇA DA GESTORA

7.1. COMITÊ DE INVESTIMENTOS

Compete ao Comitê de Investimentos a supervisão e a governança das teses e tomadas de decisão de investimentos da Gestora.

- Aprovar a política de investimentos dos fundos e carteiras sob gestão;
- Rever periodicamente os parâmetros de alocação, critérios de elegibilidade e restrições legais, regulatórias ou mandatárias (enquadramento pré-*trade*);
- Garantir tratamento equitativo entre os fundos e carteiras administradas quando verificarem oportunidades de investimentos adequadas a mais de um fundo ou carteira (rateio e divisão de ordens – *fair allocation*);
- Diligenciar as empresas investidas ou os ativos investidos, mantendo evidências de todo o processo de construção da tese de investimento ou de desinvestimento;
- Analisar contrapartes executantes, não somente sob a ótica de preço, mas de maneira holísticas em termos de tempestividade, qualidade de execução, alocação em eventos, relatórios etc. (melhor execução *best execution*);
- Encaminhar propostas de *soft dollar* para avaliação do Comitê de Compliance;
- Manter registro do exercício do direito de voto dos ativos pertencente aos fundos e carteiras sob gestão;
- Agir sempre no melhor interesse dos fundos e carteiras administradas;
- Reportar prontamente ao Comitê de Compliance qualquer situação de conflito de interesses dos membros e dos ativos investidos;
- Fazer cumprir o dever de fidúcia.

O Comitê de Investimentos é composto por 3 (três) membros: o CIO / CEO e COO podendo haver membros convidados. As reuniões serão consideradas válidas com a presença de todos os membros, poderão ocorrer de forma presencial ou online e, quando necessário, serão registradas em atas ou por e-mail interno. As reuniões do Comitê serão realizadas, ordinariamente, com periodicidade bimestral e, extraordinariamente, sempre que necessário, mediante convocação de qualquer de seus membros, em especial do Diretor de Investimentos.

Relacionamento com o Comitê de Compliance

- Compartilhar informações estratégicas com o Comitê de Compliance, especialmente no que tange a conflitos de interesse, enquadramento de ativos e situações de exceção;
- Havendo dúvidas, validar que as decisões de investimento estejam compatíveis com as normas vigentes e as políticas da gestora.

7.2. COMITÊ DE RISCO

Compete ao Comitê de Riscos a supervisão e a governança dos limites dos fatores de riscos aos quais os fundos e carteiras administradas pela Gestora estejam sujeitos. Fazem parte do Comitê de Riscos: o Diretor de Risco / CEO e COO, podendo haver membros convidados. As reuniões serão consideradas válidas com a presença de todos os membros, poderão ocorrer de forma presencial ou online e, quando necessário, serão registradas em atas ou por e-mail interno. As reuniões do Comitê serão realizadas, ordinariamente, com periodicidade bimestral e, extraordinariamente, sempre que necessário, mediante convocação de qualquer de seus membros, em especial do Diretor de Risco.

- Supervisão da estrutura da Gestão de Risco da Gestora;
- Monitorar a efetividade do sistema de gerenciamento de riscos da gestora e dos fundos e carteiras sob gestão;
- Avaliar a aderência dos controles às políticas de investimento e aos limites de enquadramento dos fundos e carteiras administradas;
- Avaliar a aderência às políticas internas de risco, limites operacionais e normas regulatórias (CVM, ANBIMA, CMN);
- Revisar periodicamente os métodos e modelos adotados para mensuração e controle de risco;

- Analisar exposições a risco de mercado: volatilidade, *duration*, alavancagem, concentração e sensibilidade a fatores de risco (ex: variações de juros, câmbio, inflação);
- Acompanhar métricas como VaR, *tracking error*, beta, sensibilidades e *backtesting*;
- Avaliar os efeitos de mudanças de cenário sobre as carteiras e recomendar ajustes;
- Avaliar a capacidade de liquidação dos ativos frente aos passivos dos fundos;
- Analisar indicadores como: perfil de vencimento, liquidez esperada *versus* resgates potenciais, e classificação de ativos por níveis de liquidez;
- Supervisionar testes de estresse de liquidez e acompanhar simulações de cenários adversos;
- Monitorar o cumprimento de limites operacionais, incluindo:
    - Limites de exposição a ativos/contrapartes;
    - Limites de concentração setorial ou geográfica;
    - Limites de risco por veículo ou estratégia.
- deliberar sobre exceções ou casos extraordinários de desenquadramento.

Relacionamento com os Comitês de Investimentos e Compliance

- Coordenar comitês para alinhar risco assumido *versus* risco autorizado;
- Reportar desvios relevantes ao Comitê de Compliance, inclusive potenciais riscos de não conformidade;
- Compartilhar dados de risco relevantes para tomada de decisão de investimentos e para comunicação a cotistas e reguladores.

7.3. COMITÊ DE COMPLIANCE

No âmbito deste Manual, compete ao Comitê de Compliance a supervisão e a governança do Programa de Compliance da Gestora.

- Analisar e deliberar sobre as situações reportadas pelo Diretor de Compliance;
- Revisar periodicamente as metodologias, parâmetros e instrumentos de controle utilizados pela Gestora, bem como avaliar eventuais descumprimentos às disposições previstas no Código de Ética, neste Manual, nas outras políticas internas da Gestora e na regulamentação vigente aplicável a indústria de fundos e aos mercados financeiro e de capitais;
- Aprovar políticas, manuais e códigos;

- Avaliar a independência e suficiência de recursos da área de Compliance;
- Avaliar os riscos inerentes e compará-los ao ambiente de controle para identificar inadequações ou vulnerabilidades e sugerir plano de ação para corrigir ou mitigar os riscos de Compliance;
- Realizar investigações internas;
- Realizar testes de aderência às políticas internas;
- Reportar atividades suspeitas de PLD/FTP;
- Analisar, em conjunto com outras áreas, prestadores de serviços;
- Aprovar anualmente o relatório anual de controles internos e de PLD/FTP e demais relatórios regulatórios aplicáveis.

O Comitê de Compliance é composto por 3 (três) membros: Diretor de Compliance / CEO e COO podendo haver membros convidados. As reuniões serão consideradas válidas com a presença de todos os membros, poderão ocorrer de forma presencial ou online e, quando necessário, serão registradas em atas ou por e-mail interno. As reuniões do Comitê serão realizadas, ordinariamente, com periodicidade bimestral e, extraordinariamente, sempre que necessário, mediante convocação de qualquer de seus membros, em especial do Diretor de Compliance.

Destaca-se que o Diretor de Compliance detém plena autonomia funcional e hierárquica, inclusive para convocar reuniões extraordinárias do Comitê a qualquer tempo, sem qualquer subordinação à equipe de gestão de recursos, em linha com os princípios de independência e segregação de funções previstos na Resolução CVM nº 21/21.

8. SOFT DOLLAR

Todo e qualquer acordo de *soft dollar* deverá ser avaliado pelo Comitê de Compliance para fins de gestão de conflito de interesses e risco regulatório.

Para fins da Gestora e deste Manual, um acordo de *soft dollar* é considerado todo e qualquer benefício que uma gestora de recursos recebe de corretoras em troca de alocação de ordens.

Exemplos de *soft dollars*:

Serviço Recebido	**Válido como Soft Dollar?**
Relatórios de análise de ações	✅ Sim

Dados de mercado (Bloomberg, FactSet)	✅ Sim
Mobiliário de escritório	❌ Não
Viagens ou presentes	❌ Não
Sistemas de gestão de risco, backoffice e compliance	❌ Não

A Gestora, por meio de seus representantes, deverá observar os seguintes princípios ao firmar acordos de *Soft Dollar*:

(i) Colocar os interesses dos clientes acima de seus próprios interesses;
(ii) Definir de boa-fé se os valores pagos pelos clientes e, consequentemente, repassados aos Fornecedores, são razoáveis em relação aos serviços de execução de ordens ou outros benefícios que esteja recebendo;
(iii) Ter a certeza de que o benefício recebido auxiliará diretamente no processo de tomada de decisões de investimento em relação ao veículo que gerou tal benefício, devendo alocar os custos do serviço recebido de acordo com seu uso, se o benefício apresentar natureza mista;
(iv) Divulgar amplamente a clientes, potenciais clientes e ao mercado os critérios e políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses oriundos da adoção de tais práticas;
(v) Cumprir com seu dever de lealdade, transparência e fidúcia com os clientes.

Além disso, os acordos de *Soft Dollar*:

(i) Devem ser transparentes e mantidos por documento escrito;
(ii) Devem ser registrados e mantidos pela Gestora, identificando, se possível, a capacidade de contribuírem diretamente para o processo de tomada de decisões de investimento, visando comprovar o racional que levou a firmar tais acordos de *Soft Dollar*; e
(iii) Não devem gerar qualquer vínculo de exclusividade ou de obrigação de execução de volume mínimo de transações os Fornecedores, devendo a Gestora manter a todo tempo total independência para selecionar e executar com quaisquer Fornecedores, sempre de acordo com as melhores condições para seus clientes.

Ao contratar os serviços de execução de ordens, a Gestora não buscará somente o menor custo, mas o melhor custo-benefício, em linha com os critérios de *best*

execution estabelecidos no mercado internacional, devendo ser capaz de justificar e comprovar que os valores pagos aos Fornecedores com que tenha contratado *Soft Dollar* são favoráveis aos fundos de investimento e carteiras sob sua gestão comparativamente a outras corretoras, considerados para tanto não apenas os custos aplicáveis, mas também a qualidade dos serviços oferecidos, que compreendem maior eficiência na execução de transações, condições de segurança, melhores plataformas de negociação, atendimento diferenciado, provimento de serviço de análise de ações e qualidade técnica dos materiais correspondentes, disponibilização de sistemas de informação, entre outros.

Caso o benefício seja considerado de uso misto, os custos deverão ser alocados de forma razoável, de acordo com a utilização correspondente.

8.1. CONFIDENCIALIADADE

A Gestora adota rigorosos padrões de conduta em relação ao tratamento de informações privilegiadas, com o objetivo de preservar a integridade do mercado e proteger os interesses de seus clientes, em conformidade com a legislação vigente no Brasil.

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

(i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;

(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora;

(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

(v) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;

(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

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

(viii) Outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários ou jovens aprendizes da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados, 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.

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

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

8.2. PRESTAÇÃO DE INFORMAÇÕES E MATERIAIS DE DIVULGAÇÃO

Os materiais publicitários e técnicos da Gestora, dos fundos e das carteiras administradas sob gestão são elaborados conforme as normas da CVM e ANBIMA.

Qualquer Colaborador que envie uma comunicação para qualquer investidor ou investidor potencial é responsável por garantir que a comunicação tenha sido devidamente examinada através dos canais adequados.

9. SEGURANÇA DA INFORMAÇÃO

A Gestora adota uma abordagem baseada em risco para a gestão da segurança da informação, em conformidade com a norma internacional ISO/IEC 27001, os controles do NIST *Cybersecurity Framework* e as melhores práticas de mercado. Esta seção estabelece as diretrizes gerais para a proteção de informações sensíveis, tanto da própria Gestora quanto de seus clientes e partes interessadas.

Essas diretrizes aplicam-se a todas as formas de informação, incluindo mídia digital, física, escrita, verbal, visual ou qualquer outro meio tangível ou intangível. A confidencialidade, integridade e disponibilidade da informação devem ser preservadas em todo o seu ciclo de vida.

A divulgação de qualquer informação classificada como confidencial é estritamente proibida fora do escopo das atividades autorizadas da Gestora. Em contratos com terceiros que tenham acesso a essas informações, é obrigatória a inclusão de cláusulas de confidencialidade, com previsão de sanções contratuais em caso de violação

9.1. RELATÓRIOS SOBRE A GESTORA

Relatórios Institucionais, auditorias, inspeções regulatórias, avaliações de risco e relatórios de *rating* realizados por entidades externas são de propriedade da Gestora e classificados como informações confidenciais. Seu uso e armazenamento devem seguir os controles internos estabelecidos na Política de Segurança da Informação.

9.2. E-MAIL E SISTEMAS INTERNOS

O uso de sistemas eletrônicos e canais de comunicação fornecidos pela Gestora deve obedecer aos princípios de uso aceitável definidos na Política de Segurança da Informação. É expressamente proibido:

- Utilizar recursos para fins pessoais, autopromoção, *spam* ou acesso a conteúdo impróprio;
- Enviar ou receber arquivos executáveis (.exe), *scripts*, macros ou anexos potencialmente maliciosos;
- Compartilhar senhas de acesso.

O uso dos recursos corporativos deve ser realizado com responsabilidade, considerando que não há garantia de privacidade individual. Todo o tráfego poderá ser monitorado, em conformidade com as políticas internas da empresa.

9.3. PRÁTICAS PROIBIDAS: *INSIDER TRADING*, *FRONT-RUNNING* E DIVULGAÇÃO INDEVIDA

É terminantemente proibido o uso de informações privilegiadas para obtenção de vantagem financeira direta ou indireta. Isso inclui práticas como *front-running*, *insider trading* ou divulgação de dicas a terceiros. Informações sobre desempenho de ativos e composição de carteiras são consideradas confidenciais e seu acesso e compartilhamento devem respeitar a regulamentação da CVM.

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

Qualquer violação está sujeita à apuração pelo Comitê de Compliance, podendo implicar em sanções administrativas e legais, conforme previsto no Código de Ética e Conduta da Gestora.

10. TECNOLOGIA E SEGURANÇA CIBERNÉTICA

Esta seção estabelece diretrizes de segurança cibernética alinhadas às práticas da ISO/IEC 27001, NIST CSF e LGPD. Seu objetivo é garantir a resiliência dos sistemas, mitigar riscos cibernéticos e proteger os dados sensíveis sob responsabilidade da Gestora.

10.1 RISCOS INTERNOS E EXTERNOS

A Gestora realiza periodicamente avaliações de risco que identificam como principais ameaças:

- Acesso indevido a informações de investidores, clientes, funcionários e dados operacionais;
- Exposição de ativos, carteiras e estratégias de investimento;
- Comprometimento da infraestrutura tecnológica e vulnerabilidades nos sistemas;
- Deficiências nos controles de acesso e autenticação.

10.2. RISCOS CIBERNÉTICOS

Os principais vetores de risco incluem:

- *Malware* e *ransomware*;
- *Phishing*, engenharia social e coleta de credenciais;

Exploração de falhas em *softwares*, sistemas ou configurações inadequadas.

10.3. AÇÕES DE PREVENÇÃO E PROTEÇÃO

A Gestora adota medidas de proteção em camadas, incluindo:

- Conduta e proteção de dados físicos:
  - Controle estrito de acesso lógico e físico a documentos e sistemas;
  - Política de mesas limpas e bloqueio automático de telas inativas;
  - Proibição de cópias indevidas de arquivos confidenciais;
  - Classificação da informação conforme política interna (Pública, Interna, Confidencial, Restrita).

Regra geral de conduta

A Gestora controla rigorosamente o acesso a arquivos que contenham informações confidenciais em meio físico, disponibilizando-os apenas aos funcionários envolvidos diretamente.

É estritamente proibido realizar cópias físicas ou eletrônicas de arquivos confidenciais. Os funcionários devem evitar deixar documentos com informações pessoais em suas estações de trabalho ou em qualquer outro espaço físico da empresa durante ausências, especialmente após o expediente.

Ao deixar a estação de trabalho, o funcionário deve bloquear a tela.

Uso de internet e Controle de Tráfego

A Gestora implementa mecanismos de autenticação para controlar o acesso à internet de seus usuários, garantindo a titularidade de cada acesso.

Os funcionários só podem fazer download de arquivos necessários para suas atividades. O uso de software *peer-to-peer* (P2P) e acesso a sites de proxy são estritamente proibidos.

- Aplicação de filtros de conteúdo e inspeção de tráfego por *firewall* de próxima geração (NGFW);
- Restrições ao uso de ferramentas P2P, VPNs pessoais e *proxy*;
- Registro e rastreamento de sessões com autenticação vinculada a identidade digital.

Utilização do e-mail

- Monitoramento do uso do e-mail corporativo com regras DLP (*Data Loss Prevention*);
- Proibição do uso para fins não corporativos ou envio de conteúdo malicioso;
- Revogação imediata de contas de e-mail de usuários desligados;
- Política de *naming* e gestão centralizada de caixas de e-mail.

Todas as contas de e-mail terão um titular responsável por sua utilização. Contas de funcionários desligados serão bloqueadas imediatamente.

O usuário é responsável pelas mensagens enviadas através de seu endereço de e-mail e deve usá-lo de maneira profissional.

Compartilhamento em nuvem

- Utilização controlada de soluções de armazenamento (ex: Dropbox, OneDrive, Sharepoint) com segregação de acesso e logs de auditoria;
- Aplicação de política de acesso mínimo necessário (*least privilege*);
- Revalidação de acessos trimestralmente.

A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, especialmente aqueles com informações confidenciais, de acordo com as funções dos funcionários, e pode monitorar esse acesso com base nas credenciais de login.

Acesso, login e senhas

- Adoção de autenticação multifator (MFA);
- Políticas de senhas fortes e não compartilhadas;
- Bloqueio por inatividade;
- Responsabilização direta por acessos realizados sob login individual.

As senhas e logins para acessar dados em computadores e e-mails, incluindo webmail, devem ser pessoais e não devem ser compartilhadas com terceiros.

A identificação do usuário por senha é única e o torna responsável por todas as atividades realizadas.

Compartilhar senhas com terceiros é passível de responsabilização do funcionário.

Equipamentos e recursos corporativos

- Monitoramento de *endpoints* com EDR (*Endpoint Detection and Response*);
- Proibição de uso pessoal irrestrito em equipamentos corporativos;
- Aplicação de políticas em dispositivos móveis.

Cada funcionário é responsável por garantir a segurança das informações nos equipamentos sob sua responsabilidade. Os ativos e sistemas da Gestora devem ser usados principalmente para fins profissionais, e o uso pessoal deve ser evitado, não sendo prioridade em relação ao uso profissional.

Controle de acesso físico

- Crachá pessoal e intransferível para todos os colaboradores;
- Monitoramento de entradas e saídas;
- Registros de visitantes e terceiros controlados.

O acesso dos funcionários às dependências da Gestora é feito através de crachá de acesso, que é pessoal e intransferível. Cada funcionário recebe seu crachá no momento da contratação.

A utilização do crachá é indispensável para circular no ambiente de trabalho.

10.4. MONITORAMENTO CONTÍNUO E TESTES DE SEGURANÇA

A Equipe de Compliance, em conjunto com a área de Tecnologia, implementará medidas de monitoramento para detectar acessos não autorizados ou violações potenciais de dados e sistemas. Isso inclui o monitoramento por amostragem da

utilização da internet, e-mail e chamadas telefônicas, bem como o monitoramento do acesso físico ao escritório.

- Monitoramento contínuo de tráfego, autenticações, anomalias e *logs* de auditoria;
- Análise de eventos críticos com base em alertas;
- Testes anuais de penetração e simulações de resposta a incidentes;
- Testes de restauração de *backup* com periodicidade definida;
- Testes de engenharia social e campanhas de *phishing* para conscientização.
- Suspeitas de vazamento, comprometimento de rede ou violação de dados devem ser comunicadas imediatamente a Equipe de Compliance, que convocará o Comitê de Crise se necessário.

Medidas adicionais de monitoramento poderão ser adotadas conforme necessário.

Testes e periodicidade

Anualmente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam: verificação do *login* dos funcionários, testes no *firewall*, testes no *backup* diário, realizado em um HD externo além do servidor.

Identificação de suspeitas

Se houver suspeita de infecção, acesso não autorizado, comprometimento da rede ou dispositivos da Gestora, ou vazamento de informações confidenciais, o Diretor de Compliance deve convocar uma reunião extraordinária, com participação do DPO, para discutir e/ou comunicar as medidas necessárias.

Ações cabíveis

Após realizado o Comitê de Compliance com a participação do DPO, o DPO é responsável por responder a qualquer informação relacionada a suspeitas de infecção, acesso não autorizado ou comprometimento da rede ou dispositivos da Gestora.

Devem ser tomadas medidas que incluem avaliar o tipo de incidente, as informações acessadas e a extensão da perda. Identificar sistemas que precisam ser desconectados ou desabilitados e avaliar a necessidade de recuperação ou restauração de serviços prejudicados também é essencial. O Diretor de Compliance também deve avaliar a

necessidade de publicar um fato relevante ao mercado, conforme exigido pela regulamentação vigente, se necessário.

O Comitê de Compliance decidirá quem arcará com as perdas após investigar e avaliar o incidente.

10.5. RESPOSTA A INCIDENTES E COMUNICAÇÃO

Conforme diretrizes do NIST (SP 800-61), as etapas de resposta a incidentes incluem:

- Identificação e categorização do incidente;
- Contenção, mitigação e erradicação da ameaça;
- Recuperação de sistemas e continuidade operacional;
- Comunicação interna, regulatória e externa (fato relevante, se aplicável);
- Análise pós-incidente (lições aprendidas).

10.6. ARQUIVAMENTO E RETENÇÃO DE REGISTROS

Em conformidade com a LGPD e a Política de Retenção da Gestora, os documentos, registros operacionais, extratos e evidências de auditoria devem ser arquivados por, no mínimo, 5 anos, ou mais, conforme exigido pela regulamentação aplicável (ex: CVM, BACEN, SUSEP).

O armazenamento seguro deve considerar:

- Controle de acesso lógico e físico;
- Cópias de segurança (backups);
- Descarte seguro e rastreável após o período de retenção.

Todas as disposições descritas nesta seção devem ser lidas em conjunto com a Política de Segurança da Informação e Segurança Cibernética da Gestora, que detalham os controles, responsabilidades, tecnologias utilizadas e níveis de criticidade dos ativos de informação.

11. SEGREGAÇÃO DAS ATIVIDADES

A Gestora atua em três frentes reguladas e complementares: gestão de fundos de investimento exclusivos, serviços de gestão de carteira administrada e gestão patrimonial (*wealth management*). Em razão disso, adota uma estrutura organizacional cuidadosamente desenhada para garantir a segregação funcional,

física e tecnológica entre as atividades, conforme estabelecido na Resolução CVM nº 175/2022, Resolução CVM nº 21/2021, e nas diretrizes da ANBIMA.

A segregação de atividades tem como objetivo mitigar conflitos de interesse, preservar a independência das decisões e assegurar a integridade dos controles internos e da relação com investidores, cotistas e clientes.

Segregação entre as atividades da Gestora

1. **Gestão de Fundos de Investimento Exclusivos***:* A equipe de gestão é exclusivamente dedicada à gestão das carteiras de valores mobiliários dos fundos de investimento exclusivos sob gestão da Gestora e tomada de decisões de investimento. Esta área atua de forma independente, sendo vedado seu envolvimento direto com a captação de clientes ou recomendação individualizada de produtos.

2. ***Wealth Management****:* A área de *wealth management* é voltada à gestão e individualizada de carteiras administradas e patrimônios, com foco na alocação estratégica de ativos, considerando o perfil e os objetivos de cada cliente. Esta equipe não interfere nos processos de decisão da gestão de fundos nem participa da distribuição direta de produtos, mantendo assim a independência necessária entre funções consultivas e comerciais.

Segregação Física e Tecnológica

A Gestora adota políticas rígidas para assegurar que as áreas citadas acima operem de forma independente e controlada, com mecanismos como:

- Separação física entre as equipes de gestão e *wealth management*, quando aplicável;
- Acessos restritos a sistemas, servidores e arquivos digitais, conforme o perfil de atuação de cada colaborador;
- Ambientes tecnológicos isolados, com credenciais individuais, controle de permissões e rastreabilidade de acessos;

Equipamentos dedicados e uso exclusivo por colaborador, evitando o compartilhamento de informações sensíveis.

Controles, Monitoramento e Responsabilidades

A Equipe de Compliance é responsável por zelar pela efetividade dos controles de segregação, atuando com autonomia funcional e hierárquica. O Comitê de Compliance realiza o monitoramento contínuo da integridade entre as áreas, identificando e tratando potenciais situações de conflito de interesse.

Tentativas de acesso indevido, movimentações não autorizadas ou violação dos procedimentos de segregação são registradas, analisadas e, quando necessário, tratadas com medidas corretivas e disciplinares, conforme o disposto neste Manual e na política de conduta da instituição.

Com essa estrutura, a Gestora assegura que suas atividades sejam conduzidas com independência, integridade e conformidade regulatória, reforçando seu compromisso com os princípios de transparência e governança corporativa.

12. DILIGÊNCIA PARA CONTRATAÇÃO

Antes de efetivar qualquer contratação, procedemos com uma minuciosa consulta aos órgãos reguladores e autorreguladores para identificar eventuais impedimentos legais ou regulatórios. Se alguma restrição for detectada, o processo de contratação é imediatamente suspenso, permitindo ao candidato o tempo necessário para regularizar sua situação junto ao órgão pertinente.

No caso de não haver qualquer impedimento, avançamos com a contratação do candidato. Após a admissão, estabelecemos um monitoramento para assegurar não apenas a performance profissional, mas também a aderência do funcionário aos Códigos Internos da Gestora.

Esperamos e incentivamos que cada membro da equipe mantenha uma conduta exemplar e alinhada com os mais altos padrões éticos e de integridade. Essa prática de monitoramento constante reflete nosso compromisso com a transparência, a conformidade regulatória e a excelência em todos os aspectos de nossas operações.

13. TREINAMENTOS E CERTIFICAÇÕES

Após a contratação, cada funcionário passará por um treinamento para adquirir conhecimento sobre as atividades da Gestora e esclarecer eventuais dúvidas sobre regras e normas.

A Gestora fornecerá treinamento a todos os funcionários sempre que este Manual for atualizado, garantindo que permaneçam atualizados sobre as políticas e procedimentos da empresa.

O treinamento e atualização ficará a cargo do Diretor de Compliance.

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

Nesse sentido, somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA, uma vez que esta certificação é aplicável aos profissionais que atuam em carteiras administradas, fundos de investimento financeiros e/ou fundos de índice, sendo certo que, a partir de 02 de janeiro de 2026, a Gestora deverá manter, no mínimo 2 (dois) profissionais certificados, conforme detalhado adiante.

A Gestora destaca que as certificações são de cunho pessoal e intransferíveis.

Ademais, para a prestação de serviços de gestão de patrimônio foi identificado que a CEA, CGA e a CGE são as certificações pertinentes às suas atividades de gestão profissional dos ativos financeiros integrantes da carteira dos veículos de investimento, com foco individualizado nas necessidades financeiras do investidor. Adicionalmente, ainda poderão ser utilizadas, somente para fins desta atividade, as certificações CFP e CFA.

Nesse sentido, destaca-se ainda que o Regras e Procedimentos de Certificação Anbima determina que, no mínimo, 75% (setenta e cinco por cento) dos profissionais que atuam na gestão de patrimônio, realizando o contato comercial com o investidor e o assessorando em suas decisões de investimento, devem ser certificados CEA, CGA, CGE, CFP ou CFA.

13.1. IDENTIFICAÇÃO DE PROFISSIONAIS CERTIFICADOS E ATUALIZAÇÃO DO BANCO DE DADOS

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Equipe de Compliance deverá solicitar esclarecimentos ou confirmar junto ao

supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação Anbima, uma vez que, em caso positivo, a Gestora deverá inserir o Colaborador no Banco de Dados.

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

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

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

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

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

13.2. ROTINAS DE VERIFICAÇÃO

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

Ainda, o Diretor de Gestão deverá contatar a Equipe de Compliance prontamente, sempre que houver algum tipo de alteração nos cargos/funções dos Colaboradores

que integram o departamento técnico envolvido na gestão de recursos e/ou com quais produtos cada destes Colaboradores atuarem, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

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

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

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

13.3. ATUALIZAÇÃO DAS CERTIFICAÇÕES

A certificação CGA (inclusive a obtida antes de 02 de janeiro de 2026) possui prazo de validade de 5 (cinco) anos.

Portanto, previamente ao vencimento das certificações, os Profissionais Elegíveis deverão participar do procedimento de atualização estabelecido pela ANBIMA, a fim de que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos acima.

Adicionalmente, anualmente, a Equipe de Compliance, Risco e PLD realizará a verificação da vigência das certificações dos Profissionais Elegíveis para cumprimento das Regras e Procedimentos de Certificação.

As Regras e Procedimentos de Certificação Anbima determinam, ainda que as gestoras de recurso deverão manter em sua estrutura um Profissional Titular e, no mínimo, um Profissional Suplente com poder discricionário de investimento na atividade de Gestão de Recursos de Terceiros em caso de indisponibilidade transitória do Profissional Titular.

Portanto, a partir de 02 de janeiro de 2026, os Profissionais Titulares e Suplentes deverão integrar o quadro permanente de colaboradores da Gestora e atuar direta e regularmente na atividade de gestão de recursos de terceiros, sendo vedada a indicação de prestadores de serviços externos, excetuados os casos em que a prestação de serviços.

Desse modo, a Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos nas Regras e Procedimentos de Certificação.

14. MANUTENÇÃO E RETENÇÃO DE ARQUIVOS

Nos termos da RCVM 21/21 a Gestora deverá manterá, por prazo não inferior a 5 (cinco) anos, todos os documentos e informações exigidos, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções.

15. PENAS DISCIPLINARES

Ao assinar o Formulário de Declaração Inicial e Reafirmação Periódica – Manual de Compliance, que é enviado pela plataforma BRE Compliance, o funcionário declara ter ciência das Políticas, Códigos e Manuais Internos da Gestora e concorda com as regras estabelecidas.

Os Colaboradores estão cientes de que qualquer violação pode acarretar penalidades determinadas pelo Comitê de Compliance da Gestora, considerando a gravidade da infração, o cargo do funcionário e o impacto para a empresa e equipe.

As penalidades podem incluir suspensão, multa e até demissão. Todas as sanções estarão em conformidade com as leis trabalhistas do Brasil e o Colaborador será ouvido em todas as fases.

Toda e qualquer penalidade será aplicada somente após uma investigação adequada da infração cometida.

Ao assinar o Formulário de Declaração Inicial e Reafirmação Periódica – Manual de Compliance, os Colaboradores afirmam que tomaram ciência das Políticas Internas e Manuais da Gestora e concordam com as regras e princípios definidos.

ANEXO I

MODELO DO FORMULÁRIO

DECLARAÇÃO INICIAL E REAFIRMAÇÃO PERIÓDICA - MANUAL DE COMPLIANCE

Nome:

Data:

1. Declaro que recebi, li integralmente e compreendi o conteúdo do Manual de Controles Internos da **REAL WEALTH MULTI FAMILY OFFICE LTDA.** ("Gestora"), estando ciente de seus princípios, normas e diretrizes.
    - ▫ Sim
    - ▫ Não

2. Você ou algum membro de sua família imediata (cônjuge, pais e filhos) está empregado por uma empresa de serviços financeiros ou que atue no mercado de capitais diferente da Gestora?
    - ▫ Sim
    - ▫ Não

3. Você foi acusado, condenado ou declarou-se culpado ou sem contestação em um tribunal doméstico, estrangeiro ou militar por algum dos seguintes crimes: crime grave, contravenção envolvendo investimentos ou um negócio relacionado a investimentos, ou qualquer fraude, declarações falsas, omissões, apropriação indevida de propriedade, suborno, perjúrio, falsificação, contrafação, extorsão ou conspiração para cometer qualquer um desses delitos?
    - ▫ Sim
    - ▫ Não

4. Alguma agência reguladora ou autorreguladora, brasileira ou estrangeira, já emitiu uma ordem ou liminar contra você em conexão com uma atividade relacionada a investimentos ou a realização de falsas representações? Já negou, suspendeu ou revogou seu registro ou licença, ou de alguma forma o impediu, por ordem, de se associar a um negócio relacionado a investimentos ou restringiu suas atividades?
    - ▫ Sim

- ▫ Não

5. Você tem conhecimento de algum conflito de interesse envolvendo a Gestora, outros colaboradores, você ou membros de sua família imediata, e qualquer cliente ou investidor?
   - ▫ Sim
   - ▫ Não

6. Você exerce, atualmente, alguma atividade profissional remunerada além das suas funções na gestora?
   - ▫ Sim
   - ▫ Não

7. Você é considerado Pessoa Exposta Politicamente?
   - ▫ Sim
   - ▫ Não

8. Você possui relacionamento próximo com Pessoas Expostas Politicamente?
   - ▫ Sim
   - ▫ Não

9. Recebi uma cópia do Manual de Compliance ("Manual") da Gestora, cujas regras e políticas me foram previamente explicadas e em relação às quais tive oportunidade de tirar todas as dúvidas existentes, tendo ainda lido e compreendido todas as diretrizes estabelecidas no mesmo, me comprometendo a observar integralmente todas as disposições dele constantes no desempenho de minhas funções, dando total conhecimento da existência do Código, o qual recebi e mantenho em meu poder.
   - ▫ Sim
   - ▫ Não

10. Tenho absoluto conhecimento sobre o teor do Manual e comprometo-me a observá-lo integralmente, em todos os seus termos.
    - ▫ Sim
    - ▫ Não

11. Comprometo-me, ainda, a informar imediatamente a Gestora sobre qualquer fato que eu venha a ter conhecimento que possa gerar algum risco para a imagem da Gestora ou descumprimento deste Manual.
    - ▫ Sim
    - ▫ Não

12. A partir desta data, estou ciente que a não observância do Manual poderá implicar na caracterização de infrações, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive desligamento ou demissão por justa causa.
    - ▫ Sim
    - ▫ Não

13. Compreendo que as regras estabelecidas no Manual não invalidam nenhuma disposição do contrato de trabalho, ou de qualquer outra regra estabelecida pela Gestora, mas apenas servem de complemento e esclarecem como lidar com determinadas situações relacionadas à minha atividade profissional.
    - ▫ Sim
    - ▫ Não