MANUAL DE SEGREGAÇÃO DA TERRA ASSET
Data de início da Vigência: 01 de janeiro de 2026

Terra Asset - Manual de Segregação

1. OBJETIVO, ABRANGÊNCIA E BASE NORMATIVA

1.1. Objetivo. Este Manual de Segregação de Atividades ("Manual") estabelece regras, procedimentos e controles para assegurar (i) a segregação adequada de funções e atividades; (ii) a proteção de informações confidenciais e informação relevante não divulgada ao público; e (iii) a mitigação de conflitos de interesse, prevenindo fraudes, erros e riscos de conduta.

1.2. Abrangência. Este Manual aplica-se a sócios, administradores, diretores, empregados, estagiários, trainees, prepostos e prestadores de serviços ("Colaboradores") da Terra Asset ("Gestora"), devendo ser formalmente aceito mediante assinatura do Termo de Recebimento e Compromisso (Anexo I).

1.3. Base normativa (não exaustiva). Este Manual está alinhado às principais normas aplicáveis ao mercado de capitais e à atividade de administração/gestão de recursos, incluindo:

- Lei nº 6.385/1976 (mercado de valores mobiliários e competência da CVM).
- Resolução CVM nº 21/2021 (administração de carteiras de valores mobiliários) e alterações posteriores.
- Resolução CVM nº 44/2021 (informações relevantes, vedações de negociação e regras relacionadas ao uso indevido de informação).
- Resolução CVM nº 175/2022 (fundos de investimento – deveres e regras de prestação de serviços, quando aplicável).
- Lei nº 13.709/2018 (LGPD – proteção de dados pessoais) e boas práticas de segurança e privacidade.
- Lei nº 12.846/2013 (Lei Anticorrupção – integridade e prevenção de condutas ilícitas).
- Códigos ANBIMA aplicáveis (quando a Gestora for aderente), incluindo o Código de Ética e, quando aplicável, o Código de Administração e Gestão de Recursos de Terceiros – AGRT.

1.4. Princípios. A segregação e as barreiras de informação devem refletir o dever fiduciário da Gestora perante clientes e investidores, bem como os princípios de lealdade, boa-fé, transparência, confidencialidade, necessidade de conhecimento (need-to-know) e menor privilégio (least privilege).

2. DEFINIÇÕES

Para fins deste Manual, aplicam-se as seguintes definições:

- Segregação de atividades: separação organizacional, física e/ou lógica (sistemas e acessos) entre funções, processos e informações sensíveis, visando mitigar conflitos e riscos.
- Barreiras de informação (Chinese Wall): controles destinados a impedir ou limitar a circulação de informação entre pessoas/equipes quando há risco de conflito, abuso de informação ou quebra de confidencialidade.
- Informação Confidencial: toda informação não pública sobre clientes, investidores, fundos, operações, estratégias, posições, modelos, sistemas, contratos, planos, dados pessoais ou terceiros.

- Informação Relevante não Divulgada: informação potencialmente apta a influenciar decisões de investimento ou preço de ativos antes de sua divulgação ao mercado.
- Acesso: qualquer forma de consulta, uso, cópia, transmissão, compartilhamento ou armazenamento de informações, dados ou documentos.

3. SEGREGAÇÃO ORGANIZACIONAL E RESPONSABILIDADES

A Gestora deverá manter segregação adequada de funções, evitando acúmulo de atribuições incompatíveis. As responsabilidades devem ser claramente definidas em organograma e descrições de função, com segregação mínima entre: (i) gestão (tomada de decisão de investimento); (ii) controles (compliance, risco, PLD/FTP quando aplicável); (iii) operações/administrativo; e (iv) tecnologia/segurança.

3.1. Diretor de Compliance e Risco

O Diretor/Responsável por Compliance e Risco é responsável por definir, supervisionar e testar os controles de segregação, avaliar exceções e aprovar acessos excepcionais, mantendo registros e justificativas. O Compliance possui autonomia técnica e deve ter acesso às informações necessárias para monitoramento.

3.2. Responsabilidades dos Colaboradores

- Cumprir este Manual e demais políticas correlatas.
- Respeitar restrições de acesso e não tentar contornar controles (por exemplo, compartilhamento de credenciais).
- Reportar imediatamente ao Compliance qualquer falha, suspeita de vazamento, acesso indevido ou conflito potencial.

4. SEGREGAÇÃO FÍSICA (INSTALAÇÕES) E CONTROLE DE ACESSO

4.1. Regra geral. O acesso às áreas de trabalho deve ser limitado aos Colaboradores autorizados. Visitantes e terceiros somente poderão acessar instalações mediante autorização prévia, registro e acompanhamento.

4.2. Área de gestão. A área utilizada pela equipe de gestão deve permanecer segregada das áreas responsáveis por outras atividades relacionadas ao mercado de capitais (caso existam), de forma a mitigar conflitos de interesse e proteger informações sensíveis.

- Controle de acesso físico (quando aplicável): chaves, cartões, biometria ou lista de autorizados.
- Política de mesa limpa (clean desk) e tela protegida (screen lock) ao se ausentar.

4.3. Trabalho remoto. Em regime remoto, os Colaboradores devem assegurar que terceiros (inclusive familiares) não tenham acesso a telas, documentos ou chamadas. Recomenda-se uso de fones, ambientes reservados e bloqueio automático de tela.

5. SEGREGAÇÃO LÓGICA (SISTEMAS), PERFIS E ACESSO A DADOS

5.1. Princípios. O acesso a sistemas, pastas e bases de dados deve obedecer aos princípios de menor privilégio (least privilege) e necessidade de conhecimento (need-to-know), com trilhas de auditoria quando aplicável.

- Autenticação multifator (MFA) sempre que disponível.
- Proibição de compartilhamento de logins/senhas; credenciais são pessoais e intransferíveis.
- Classificação de informação e segregação por pastas com permissões (ex.: clientes, fundos, jurídico, RH, modelos).

5.2. Acessos privilegiados. Acessos administrativos (TI) devem ser controlados, concedidos apenas quando necessário, e registrados. Atividades com acesso privilegiado devem ser monitoradas na medida do possível.

6. BARREIRAS DE INFORMAÇÃO (CHINESE WALL)

6.1. Finalidade. As barreiras de informação visam impedir o fluxo indevido de informações entre pessoas/equipes quando exista risco de: (i) conflito de interesses; (ii) uso indevido de informação relevante não divulgada; (iii) quebra de confidencialidade; (iv) violação de dever fiduciário.
6.2. Implementação. As restrições de acesso respeitam o organograma funcional e os perfis de acesso. Exceções podem ser avaliadas pelo Diretor de Compliance e Risco mediante solicitação formal e justificativa, com registro de: escopo, duração, motivo, controles compensatórios e responsável.

- Restricted list (lista restrita): ativos/emitentes/contrapartes com restrição de negociação e/ou de circulação de informação.
- Blackout (períodos de bloqueio): vedação temporária de negociações/compartilhamento em situações específicas.
- Separação de documentos: pastas segregadas e permissões restritas.
- Protocolos de reunião: quando necessário, limitar participantes e registrar pauta/decisões; proibir gravações não autorizadas.

7. CONFIDENCIALIDADE, SIGILO E PROTEÇÃO DE DADOS (LGPD)

7.1. Dever de confidencialidade. É proibida a divulgação de Informações Confidenciais a terceiros, para benefício próprio ou de terceiros, independentemente de intenção. O dever de confidencialidade permanece mesmo após o desligamento do Colaborador.

7.2. Pedidos de quebra de sigilo. Solicitações de órgãos públicos, reguladores e do Poder Judiciário devem ser encaminhadas ao Compliance e/ou Jurídico para validação e resposta nos estritos limites da ordem recebida.

7.3. Proteção de dados pessoais. O tratamento de dados pessoais deve observar a LGPD e as políticas internas, incluindo princípios de finalidade, necessidade, segurança e responsabilização. Compartilhamentos devem ocorrer apenas com base legal e com salvaguardas contratuais.

- Proibição de envio de dados de clientes/empresas investidas a terceiros sem autorização/base legal.
- Uso de ferramentas corporativas aprovadas para armazenamento e compartilhamento.

- Reporte imediato de incidentes envolvendo dados pessoais e/ou vazamento de informações.

8. SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

A segurança da informação visa proteger a Gestora contra ameaças e assegurar continuidade de negócios. Os controles devem ser observados por todos os Colaboradores, inclusive em ambiente remoto.

8.1. Condutas proibidas/risco elevado

- Acessar sites e instalar softwares não relacionados às atividades e não aprovados.
- Utilizar mídias removíveis (pen-drives, HDs externos) para armazenar/transportar informações sensíveis, salvo exceções aprovadas e criptografadas.
- Salvar informações confidenciais em pastas públicas ou contas pessoais não autorizadas.
- Salvar arquivos pessoais na rede institucional.
- Transportar informações não criptografadas.
- Compartilhar senhas ou desativar mecanismos de segurança.

8.2. Controles mínimos esperados

- Antivírus/EDR e atualizações de sistema.
- MFA e gestão de senhas.
- Criptografia quando aplicável.
- Proteção contra phishing (treinamento e alertas).
- Backups e controle de versões em repositórios autorizados.
- Plano de resposta a incidentes e comunicação interna.

8.3. Terceirização de TI. Caso serviços de TI sejam terceirizados, a contratação e supervisão devem observar diligência prévia, cláusulas de confidencialidade e LGPD, SLAs e requisitos de segurança compatíveis com o risco, conforme Manual de Compliance da Gestora.

9. MONITORAMENTO, TESTES E EVIDÊNCIAS

O Compliance deve monitorar e testar periodicamente a efetividade dos controles de segregação e barreiras de informação, incluindo revisões de acesso, verificação de exceções, análise de incidentes e testes de contingência. Todos os testes devem gerar evidências auditáveis.

10. REPORTE, INVESTIGAÇÕES, PENALIDADES E NÃO RETALIAÇÃO

10.1. Reporte obrigatório. Todo Colaborador deve informar imediatamente ao Diretor de Compliance e Risco qualquer violação ou suspeita de violação deste Manual, incluindo acesso indevido, vazamentos, tentativa de obtenção de informação, ou falhas de controles.

10.2. Investigações. O Compliance conduzirá (ou coordenará) a apuração com confidencialidade, preservação de evidências e respeito ao devido processo interno. Quando necessário, poderá envolver consultoria externa, TI e/ou assessoria jurídica.

10.3. Não retaliação. É expressamente vedada qualquer forma de retaliação contra Colaborador que reporte, de boa-fé, suspeitas ou violações. A retaliação constitui infração grave sujeita a sanções.

10.4. Penalidades. O descumprimento deste Manual pode resultar, conforme gravidade e reincidência: (i) advertência por escrito; (ii) suspensão; (iii) desligamento; e/ou (iv) outras medidas cabíveis. No caso de empregados, podem ser aplicadas medidas trabalhistas conforme legislação aplicável (incluindo, quando cabível, art. 482 da CLT).

11. DISPOSIÇÕES FINAIS

Este Manual será revisado, no mínimo, anualmente, ou sempre que houver mudança regulatória/material relevante. Exceções somente poderão ocorrer mediante aprovação formal do Diretor de Compliance e Risco e registro de justificativa e controles compensatórios.

Anexo I

Termo de Recebimento e Compromisso

Por meio deste instrumento eu, _____, inscrito no
CPF/ME sob o no _____, DECLARO para os devidos fins:

- Ter recebido, na presente data, o Manual de Segregação atualizado da TERRA ASSET. ("Gestora");
- Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Código;
- Estar ciente de que o Código como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e
- Estar ciente do meu compromisso de comunicar ao Diretor de Compliance e Risco da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Código.

[local], [data].

_____

[COLABORADOR]