SARFATY ASSET GESTÃO DE RECURSOS LTDA

47.813.099/0001-04

POLÍTICA DE KNOW YOUR CLIENT

(CONHEÇA SEU CLIENTE)

Janeiro 2026

É vedada a cópia, reprodução, alteração e distribuição desse documento sem prévia e expressa autorização da Sarfaty Asset Gestão de Recursos LTDA.

1. Introdução e Objetivo

A presente Política de Conheça seu Cliente ("Know Your Customer" – KYC) estabelece princípios, diretrizes e procedimentos mínimos a serem observados antes e durante todo relacionamento com o cliente, investidores, cotistas, cedentes, sacados, contrapartes e demais partes relacionadas perante as empresas abrangidas pelo Grupo Sarfaty ("Instituição"), com vistas a:

i. Identificar, qualificar, verificar e validar informações cadastrais.

ii. Identificar beneficiários finais, controladores, representantes, administradores e procuradores.

iii. Classificar e gerir riscos de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP).

iv. Estabelecer monitoramento contínuo e revisões periódicas, compatíveis com o risco.

v. Assegurar a manutenção, a armazenagem e a rastreabilidade de registros de clientes, beneficiários finais e demais partes relacionadas, cumprindo a legislação vigente e, em especial, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e a Resolução CVM nº 50/2021.

Todos os colaboradores, administradores, sócios, prepostos e prestadores de serviços contratados por quaisquer empresas abrangidas pelo Grupo Sarfaty devem observar e cumprir esta Política, atentando-se para informações claras, verídicas, completas, diligentes, precisas e atuais, mantendo-se evidências adequadas.

É vedado iniciar o relacionamento, realizar qualquer tipo de operação, pagamento ou liberar recurso, sem que o procedimento de "conheça seu cliente" esteja finalizado, atualizado e documentado, salvo hipóteses expressamente previstas na regulamentação aplicável e mediante aprovação formal da área de Compliance, Controles Internos e alçada competente, com registro de justificativa e controles mitigatórios proporcionais ao risco.

As sociedades que integram o Grupo Sarfaty devem assegurar, no mínimo, que:

i. Conhecem o cliente, sua estrutura de controle e propriedade, quem controla a sociedade ou companhia, seus representantes, administradores, procuradores, quem se beneficia e eventuais Pessoas Expostas Politicamente, bem como compreendem a finalidade, a natureza e, quando aplicável, a destinação dos recursos captados junto ao Grupo Sarfaty e a origem do patrimônio.

ii. Mantêm os dados e evidências monitorados e atualizados, com reavaliação de riscos e perfil.

iii. Cumprem com os deveres de comunicação de operações, situações suspeitas ou atípicas, reportando às autoridades competentes dentro dos prazos legais e regulatórios, resguardando o dever de sigilo, segurança da informação e de proteção dos dados pessoais.

iv. Realizam a identificação da atividade econômica do cliente e da origem dos recursos, bem como, quando aplicável e proporcional ao risco, a constituição do patrimônio do cliente.

v. Mantêm o registro, evidência e análise de operações, situações suspeitas ou atípicas de seus clientes, bem como a manutenção de arquivos, cadastro, decisões e medidas mitigatórias adotadas ao caso, sendo garantida a pronta disponibilização às autoridades competentes e aos órgãos regulatórios, quando aplicável e solicitado.

2. Definições

Para fins desta Política, considera-se:

a) Beneficiário Final: pessoa natural que controla ou exerce influência significativa, direta ou indiretamente, em nome de um cliente, seja esta pessoa natural ou jurídica, para o qual a transação esteja sendo conduzida ou dela se beneficie.

b) Cadastro: registro das informações dos clientes e partes relacionadas com os quais esta instituição mantém relacionamento direto em função da prestação de serviço, seja por meio físico ou eletrônico.

c) Cliente: pessoa natural ou jurídica que mantenha relacionamento com sociedades do Grupo Sarfaty, incluindo contratantes, cotistas, investidores, tomadores, cedentes, sacados e contraparte dos direitos creditórios cedidos em favor do Grupo, seja este residente ou não no país.

d) Influência Significativa: situação em que uma pessoa natural, seja controladora ou não, interfira nas tomadas de decisões de pessoas naturais ou jurídicas, ou seja titular direta ou indiretamente de mais de 25% do capital social das pessoas jurídicas ou do patrimônio líquido do fundo e demais entidades relacionadas, em observância à legislação aplicável.

e) Monitoramento: avaliação contínua e periódica da política, dos clientes, dos perfis e das informações relevantes e arquivadas, incluindo a seleção e análise de operações ou situações suspeitas ou atípicas, bem como classificação do risco.

f) Pessoa Exposta Politicamente (PEP): pessoa natural que desempenhe ou tenha desempenhado, nos últimos 05 (cinco) anos, seja em território nacional ou no estrangeiro, cargo, ocupação, emprego, função pública considerada relevante ou semelhante, ou mandato eletivo, bem como seus familiares em linha direta ou colateral ou pessoas com vínculo a si ou relacionamentos próximos, inclusive por meio de participação societária ou sociedade conjunta em pessoa jurídica de direito privado. Considera-se, ainda, Pessoa Exposta Politicamente, a pessoa natural que controle pessoa jurídica ou arranjo sem personalidade jurídica criado para benefício da PEP.

g) Sanções: medidas restritivas impostas por resoluções do Conselho de Segurança das Nações Unidas (CSNU) e pelos mecanismos internos de cumprimento de sanções no Brasil, incluindo indisponibilidade de ativos, nos termos da legislação aplicável. Para fins de gestão de risco e integridade, devem ser consideradas, adicionalmente, as exposições a lista restritivas e cadastro públicos, incluindo, sem limitação, Cadastro de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP), Foreign Corrupt Practices Act (FCPA) e por regimes sancionatórios aplicáveis.

h) Alerta: registro interno gerado por regra, parametrização, apontamento de área ou evento que indique a necessidade de análise de potencial operação ou situação suspeita ou atípica.

3. Abrangência

Esta Política aplica-se a todas as empresas do Grupo Sarfaty que estejam em território nacional ou no estrangeiro, seja controlada, coligada, administrada ou sob direção comum, alcançando seus sócios, colaboradores, procuradores, administradores, prepostos, prestadores de serviços que atuem em quaisquer etapas do ciclo de vida do relacionamento com o cliente e toda pessoa natural ou jurídica vinculada ao Grupo cuja atuação possa impactar o cumprimento de obrigações de Prevenção à Lavagem de Dinheiro, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP).

As áreas de Compliance e Controles Internos são responsáveis pelo cumprimento, orientação, supervisão e teste desta Política, devendo assegurar que todas as pessoas envolvidas cumpram e tenham ciência do teor apresentado.

4. Operações ou Situações Suspeitas

Como forma de padronizar e orientar os colaboradores, prestadores de serviços, prepostos, sócios, administradores e demais pessoas naturais que compõem o Grupo Sarfaty, consideram-se, de forma exemplificativa, eventos que devem ser registrados e analisados como operações ou situações suspeitas:

i. Informações falsas, inverídicas, inconsistentes, imprecisas ou documentos com indícios de adulteração;

ii. Informação de difícil verificação ou resistência injustificada do cliente em fornecer dados ou documentos mínimos;

iii. Abertura, movimentação de contas, cessões ou realização de operações por procurador ou pessoa que detenha outro tipo de mandato, sem a devida justificativa;

iv. Múltiplos cadastros e contas bancárias, em um curto espaço de tempo, sem a devida justificativa;

v. Operações em que não seja possível ou de difícil identificação do beneficiário final;

vi. Procuradores ou Representantes que possuem relações ou vínculo em diversas pessoas jurídicas ou organizações;

vii. Situações em que não seja possível manter o cadastro atualizado;

viii. Situação financeira, movimentação de recurso ou atividade econômica incompatível com a ocupação profissional declarada pelo cliente;

ix. Atividade econômica, faturamento e objeto social incompatível com o padrão operacional;

x. Operações realizadas entre as mesmas partes ou em benefício das mesmas partes;

xi. Registro de mesmo endereço de correio eletrônico ou de internet protocol (IP) por diferentes pessoas jurídicas, pessoas naturais ou organizações, sem a devida justificativa;

xii. Informações e documentos apresentados pelo cliente em que esteja conflitante com as informações públicas disponíveis;

xiii. Sócio ou controlador sem capacidade financeira aparente para compatível com o porte de atividade empresarial declarada;

xiv. Movimentação de recursos de valores elevados, de forma corriqueira, em favor de terceiros;

xv. Transferência de valores que estejam um pouco abaixo do limite para notificação ou fracionadas para evitar controles;

xvi. Agente público que abre conta, homologa junto aos fundos, vincula ou cadastra em nome de um familiar ou empresa, depositando valores elevados ou operações financeiras sem a comprovação da origem do recurso;

xvii. Ameaça, intimidação ou pressão a qualquer colaborador ou prestador de serviço para que não faça o devido reporte, controle ou anotação;

xviii. Ativos alcançados por sanções impostas pela resolução do Conselho de Segurança das Nações Unidas (CSNU);

xix. Pessoas que tenham cometido, participado, facilitado ou tentado cometer atos terroristas;

xx. Operações com a participação de pessoas naturais, pessoas jurídicas ou outra entidade que não seguem as recomendações do GAFI/FATF;

xxi. Pagamentos habituais a fornecedores ou beneficiários sem ligação com a atividade ou ramo de negócio da pessoa jurídica;

xxii. Pagamentos ou transferência por pessoa jurídica para fornecedor distante de seu local de atuação, sem justificativa;

xxiii. Utilização de instrumento financeiro de forma a ocultar patrimônio ou evitar a realização de bloqueios judiciais;

xxiv. Alteração repentina do padrão de vida do cliente, sem a devida justificativa;

xxv. Alteração repentina do resultado da sociedade ou da companhia;

xxvi. Uso de empresas de fachada, organização societária de difícil visualização;

xxvii. Sócio formalmente indicado nos atos societários, mas que não seja o de fato;

xxviii. Pessoa natural ou jurídica submetida a sanções internacionais ou constando de listas restritivas relevantes, como por exemplo Office of Foreign Assets Control (OFAC), União Europeia ou Reino Unido, conforme aplicável;

xxix. Oferecimento de vantagens ou presentes, pecuniárias ou não, aos colaboradores;

xxx. Notícias desabonadoras na mídia;

xxxi. Desenquadramento reiterado do perfil histórico;

xxxii. Jurisdições de alto risco ou de baixa cooperação internacional em matéria de PLD/FTP;

xxxiii. Transferência de recursos para Organizações Não Governamentais (ONGs) ou entidades filantrópicas sem justificativa adequada ou com finalidade pouco clara, especialmente quando incompatível com o perfil do cliente ou com histórico transacional;

xxxiv. Organização Não Governamental (ONG) e Entidades Filantrópicas;

Estas hipóteses não configuram rol taxativo e não implicam, por si sós, imputação de crime ao cliente. Constituem, entretanto, sinais de alerta que demandam análise administrativa e diligência proporcional ao risco, com documentação em dossiê. Caso seja caracterizada suspeição, a operação ou situação deverá ser comunicada ao Conselho de Controle de Atividades Financeiras (COAF) e, quando aplicável, ao órgão supervisor

competente, como por exemplo a Comissão de Valores Mobiliários (CVM), Banco Central do Brasil (BACEN), Superintendência de Seguros Privados (SUSEP) e ao Ministério da Justiça e Segurança Pública (MJSP).

5. Avaliação Interna do Risco

O comitê de Riscos e Compliance e os departamentos estruturados nos controles internos deverão, no limite de suas atribuições, identificar, recusar, analisar, comunicar ou mitigar os riscos relacionados a cada cliente e às operações a ele associadas, emitindo o seu parecer, adotando uma Abordagem Baseada em Risco (ABR) e classificando minimamente cada cliente como baixo, médio e alto risco de envolvimento em atividades relacionadas à LD/FTP.

Caso seja necessário, e nos limites de sua atribuição, a área competente poderá solicitar documentações complementares, realizar visitas conjuntas aos clientes ou requer demais esclarecimentos sobre determinado ponto considerado de alerta.

Na hipótese de não ocorrência de operações ou situações suspeitas ou atípicas passíveis de comunicação, no período de 01 (um) ano, a área de Compliance providenciará a comunicação ou declaração anual de não ocorrência, na forma e nos prazos previstos na regulamentação aplicável ao segmento da instituição, com registro interno e evidência de envio, quando exigível.

Na eventualidade de a análise concluir pela caracterização de suspeição, o comitê, em conjunto com a administração desta instituição e por meio do seu Diretor de Compliance, comunicará, no prazo não superior ao de 24 (vinte e quatro) horas a contar da elaboração do dossiê, à autoridade competente para as devidas providências ou em até 45 (quarenta e cinco) dias da data da geração do Alerta, quando aplicável o regime da Circular BCB Nº 3.978/2020.

Em caso de conflito, coexistência ou divergência normativa quanto a prazos, formas, hipóteses e destinatários de comunicação, a Instituição observará o regime aplicável ao seu segmento e ao ente regulador competente, aplicando-se, quando houver sobreposição de regramentos, o critério mais restritivo e de maior diligência.

As comunicações conterão, no mínimo:

I. A data de início do relacionamento perante esta instituição;
II. A descrição dos sinais de alerta;
III. Operação em que o cliente pretendia realizar ou realizou, apresentando todo o escopo suspeito;
IV. Qualificação dos envolvidos e seu comportamento;
V. Relato fundamentado sobre a situação suspeita a ser comunicada;
VI. Número de operações efetuadas durante todo o relacionamento.

As informações colhidas, tratadas e incluídas na comunicação deverão permanecer sob sigilo, sendo expressamente vedado a ciência às pessoas envolvidas ou a terceiros, sob pena de responsabilidade civil, administrativa e criminal, nos termos da legislação aplicável.

6. Cadastro do Cliente

A área de cadastro será responsável pela inserção, reporte, guarda, análise dos dados e dos documentos encaminhados, assim como seguir as diretrizes, treinamentos, políticas e normas internas definidas.

Caso seja identificada qualquer ação considerada suspeita, a área de Cadastro comunicará e enviará as documentações pertinentes à área de Compliance, que iniciará os procedimentos cabíveis de análise e investigação.

Até o término das investigações pela área de Compliance, a área de Cadastro não poderá concluir, habilitar, liberar, seguir, autorizar, influenciar, abrir ou homologar o cliente junto ao Grupo Sarfaty.

Caso o cliente seja Pessoa Exposta Politicamente, a área de cadastro deverá adotar diligências adicionais em sua análise.

A instituição deverá manter a guarda, integridade, rastreabilidade e pronta recuperação dos documentos, dados e informações coletadas dos clientes, bem como dos registros de operações e dossiês de análise, pelo prazo mínimo de 10 (dez) anos, ressalvadas as hipóteses legais que determina ao contrário.

6.1 Documentações mínimas necessárias a serem encaminhadas para área de cadastro:

6.1.1. Para pessoa natural:

I. Nome completo;
II. Data de nascimento;
III. Nacionalidade e naturalidade;
IV. Estado Civil e a respectiva documentação comprobatória;
V. Documentação do cônjuge, se aplicável;
VI. Comprovante de residência atualizado;
VII. Documento de identidade (RG, CPF, Passaporte e CNH);
VIII. Profissão;
IX. Endereço eletrônico;
X. Ficha cadastral preenchida;
XI. Declaração atestando a veracidade, completude e licitude das informações prestadas;
XII. Declaração de desimpedimento;
XIII. Telefone.

6.1.2. Para pessoa jurídica:

I. Nome empresarial;
II. Inscrição CNPJ;
III. Contrato social, Estatuto social e demais atos societários;
IV. Documentações financeiras, tais como, mas sem se limitar a: Faturamento, Balanço Contábil, Balancete, DRE e demais documentos financeiros relacionados à empresa;
V. Organograma societário, quadro societário e cadeia de controle;
VI. Identificação do beneficiário final.

Nos casos de Estruturas Complexas, múltiplas camadas, jurisdições de risco, entes despersonalizados, *trusts*, arranjos análogos ou quando houver indícios de ocultação, deverá ser exigida diligência reforçada e aprovação da área de Compliance.

7. Avaliação de Risco dos Clientes (Abordagem Baseada em Risco)

Esta seção estabelece critérios mínimos para a classificação do risco de clientes e de partes relacionadas, bem como as medidas de diligência e de monitoramento, com vistas à prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP).

A classificação observará o princípio da proporcionalidade e a abordagem baseada em risco, com fundamento em informações cadastrais, documentais, comportamentais, reputacionais e transacionais, em rol exemplificativo. A ocorrência de um ou mais fatores poderá ensejar a reclassificação imediata, a qual deverá ser devidamente registrada em dossiê, com indicação do fundamento e do responsável.

Com a finalidade de orientar as pessoas que compõem o Grupo, prestadores de serviços e demais entidades relacionadas, apresentam-se, a seguir, de forma não exaustiva, as medidas mínimas a serem adotadas conforme a classificação de risco aplicável.

RISCO	**CLIENTE**	**AÇÃO**
ALTO	▪ Pessoa Exposta Politicamente, seus familiares em linha reta e colaterais até 2º grau e estrito colaborador. ▪ Organização Não Governamental e Entidades Filantrópicas. ▪ Pessoa natural ou jurídica sancionada ou relacionada na lista de restrição ▪ Pessoa natural ou jurídica envolvida, citada ou condenada em esquema de corrupção, lavagem de dinheiro ou de	▪ Atualização cadastral com periodicidade máxima de 02 (dois) meses, ou em prazo inferior quando houver evento relevante. ▪ Recusa no relacionamento, conforme o caso.

	Financiamento do terrorismo e proliferação de armas de destruição em massa nos últimos 05 (cinco anos). ▪ Notícia midiática desabonadora ou que cause prejuízo para o Grupo Sarfaty em iniciar ou manter o relacionamento. ▪ Ocultação do beneficiário final ou do patrimônio. ▪ Fraude em documentação financeira, de identidade ou societária. ▪ Cliente condenado em processo sancionador da CVM nos últimos 05 (cinco anos) por falha em controles internos, compliance e LD/FTP. ▪ Cliente situado em jurisdição de alto risco ou de baixa transparência. ▪ Cliente que não possui política ou métodos de prevenção à lavagem de dinheiro e ao financiamento do Terrorismo. ▪ Cliente com modelo de negócio considerado de alto risco para LD/FTP ▪ Entidade despersonalizada ou que dificulte a origem ou destinação dos recursos ▪ Documentação financeira não auditada e desatualizada. ▪ Recusa injustificada em assinar cláusula de anticorrupção, suborno, peculato, lavagem de dinheiro, do financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa. ▪ Cliente condenado em processos penais ou administrativos de significativa relevância.	▪ Comunicação às autoridades competentes, conforme o caso. ▪ Visita *"in loco"* na sociedade, companhia ou, conforme o caso, na residência do cliente, seu representante ou procurador. ▪ Monitoramento contínuo sobre as atividades do cliente. ▪ *"Due Diligence detalhada"* com periodicidade máxima de até 03 (três) meses. ▪ Solicitação de documentações complementares e parecer técnico fundamentado da área responsável.
MÉDIO	▪ Política de PLD/FTP existente, mas se encontra desatualizada.	▪ Atualização cadastral com periodicidade

	▪ Documentação societária ou financeira desatualizada em até 01 (um) mês. ▪ Processos judiciais ou administrativo que não seja considerada grave ou prejudicial ao "Grupo Sarfaty", devendo ser analisada conforme o caso. ▪ Ramo de atividade empresarial que possa ser suscetível, de maneira mínima ou média, a LD/FTP.	máxima trimestral (no máximo a cada 03 (três) meses), ou em prazo inferior quando houver evento relevante. ▪ Requerimento de documentação complementar quando aplicável. ▪ Visita "*in loco"* na sociedade, companhia ou, conforme o caso, na residência do cliente, seu representante ou procurador ou reunião via telepresencial. ▪ *"Due Diligence detalhada",* com periodicidade máxima trimestral (no máximo a cada 03 (três) meses).
BAIXO	▪ Identificação clara dos beneficiários finais e da estrutura societária do cliente. ▪ Cliente sem mídia desabonadora. ▪ Documentação válida e auditável, conforme o caso. ▪ Políticas de Compliance e de Controles Internos válidas e eficientes. ▪ Ausência de processos desabonadores. ▪ Cliente em jurisdição de baixo risco. ▪ Rastreabilidade do recurso ou da origem do patrimônio. ▪ Documentação financeira atualizada e auditada. ▪ Ausência de apontamento na *"Due Diligence"* realizada.	▪ Atualização cadastral com periodicidade máxima anual (no máximo a cada 01 (um) ano), podendo ser inferior, conforme situação fática. ▪ *"Due Diligence padrão"*, com periodicidade máxima anual (no máximo a cada 01 (um) ano).

8. Referência Regulatória e Legal

a) Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

b) Resolução CVM nº 50, de 31 de agosto de 2021 - Dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa – PLD/FTP no âmbito do mercado de valores.

c) Circular nº 3.978, de 23 de janeiro de 2020 - Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

d) Padrões internacionais do GAFI/FATF (40 Recomendações)

e) Resolução COAF nº 34, de 15 de abril de 2020; Revoga a Resolução nº 24, de 16 de janeiro de 2013, do Conselho de Controle de Atividades Financeiras – Coaf, que dispõe sobre os procedimentos a serem adotados pelas pessoas físicas ou jurídicas não submetidas à regulação de órgão próprio regulador que prestem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, na forma do § 1º do art. 14 da Lei nº 9.613, de 3 de março de 1998, nas operações de que trata o inciso XIV do parágrafo único do seu art. 9º.

f) Resolução COAF nº 36, de 10 de março de 2021; disciplina a forma de adoção de políticas, procedimentos e controles internos de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa que permitam o atendimento ao disposto nos arts. 10 e 11 da Lei nº 9.613, de 3 de março de 1998.

g) Lei nº 13.810, de 8 de março de 2019, dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

h) Lei nº 9.613, de 3 de março de 1998, dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências.

i) Resolução BCB Nº 344, de 4 de outubro de 2023, altera a Circular nº 3.978, de 23 de janeiro de 2020, que dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de

março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

9. Canal de Denúncia

Qualquer colaborador, diretor, preposto, procurador, prestador de serviços, parceiros ou parte relacionada poderá, de boa-fé, comunicar qualquer intercorrência, irregularidade, desvio, inconformidade, indícios de violação a esta Política e demais normas internas, inclusive indícios relacionados a PLD/FTP ou condutas antiéticas, por meio dos canais abaixo:

i. e-mail: canaldenuncia@gruposarfaty.com.br;

ii. sítio eletrônico: https://gruposarfaty.com.br/contato/; ou

iii. chat: canaldenuncia@gruposarfaty.com.br

A ocorrência deverá ser registrada, receberá o número de protocolo e será submetida à triagem e tratamento pela área responsável, com preservação de confidencialidade, segurança da informação, proteção de dados pessoais e vedação de retaliação ao comunicante, bem como deverá ser atendida com a devida diligência.

Deverá ser assegurada ao comunicante, proteção contra qualquer forma de retaliação, sendo vedada qualquer tentativa de represália, direta ou indiretamente, inclusive por meio de constrangimento, discriminação, intimidação ou prejuízo profissional. Será admitida a denúncia anônima, quando disponível e aplicável, devendo ser observado o dever de sigilo e de confidencialidade quanto à identidade do comunicante, ao teor do relato e às informações dele decorrentes, com acesso restrito exclusivamente às pessoas autorizadas, na estrita necessidade de conhecimento.

10. Endereço Eletrônico e Contato

10.1 A presente política poderá ser acessada a qualquer momento no seguinte endereço eletrônico: https://gruposarfaty.com.br/.

10.2 Quaisquer dúvidas relacionadas a essa Política poderão ser endereçadas ao gestor através do correio eletrônico: gestaodefundos@gruposarfaty.com.br e Compliance@gruposarfaty.com.br.

11. Vigência e Atualização

1.1 A presente política será revisada anualmente e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo em decorrência de: (i) mudanças

regulatórias e eventuais deficiências encontradas; e (ii) testes de aderência/eficácia das métricas e procedimentos aqui previstos.

11.2 Essa política revoga todas as versões anteriores e passa a vigorar a partir da data de sua aprovação pelo Comitê de Riscos e de Compliance.

11.3 Controle de Versão:

Data	**Versão**	**Responsável**
20/01/26	1.0	Diretoria de Gestão e Diretoria de Compliance, Risco e PLD/FTP.