Política Institucional		
Área Gestora **Compliance e Gestão de Riscos**	Código	Versão **03**
Assunto **Manual de Controles Internos *(Compliance)***	Data Criação **13/11/2019**	Data Publicação **13/11/2019**
Abrangência **Limitada ao Grupo Onze**		

MANUAL DE CONTROLES INTERNOS *(COMPLIANCE)*

Histórico de Versões

Versão	Atualizada em	Alterações	Responsável:
1	Junho/2019	Criação da Política	Ricardo Domingues
2	Novembro/2020	Alteração do responsável	Mariane Akemi Hotta
3	Março/2024	Alteração do responsável	Antonio Fernando da Rocha Junior
3	Maio/2025	Revisão geral da Política	Antonio Fernando da Rocha Junior
3	Março/2026	Revisão geral da Política	Antonio Fernando da Rocha Junior

Sumário

1. INTRODUÇÃO E OBJETIVO 6
2. PROCEDIMENTOS 6
2.1. Designação de um Diretor Responsável 6
2.2. Revisão periódica e preparação de relatório 8
2.3. Treinamento 8
2.4. Apresentação do Manual de Compliance e suas modificações 8
2.5. Atividades Externas 9
2.6. Supervisão e responsabilidades 9
2.7. Sanções 9
3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO 9
3.1. Segurança da Informação Confidencial 10
3.2. Propriedade intelectual 12
4. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING 13
4.1. Insider Trading, “Dicas” e Spoofing 13
5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES 14
5.1. Segregação física 14
5.2. Segregação eletrônica 15
5.3. Especificidades dos mecanismos de controles internos 16
6. DIVULGAÇÃO DE MATERIAL DE MARKETING 17
7. APROVAÇÃO DE CORRETORAS E SOFT DOLLAR 19
7.1. Política de Soft Dollar 20
8. POLÍTICA DE KNOW YOUR CLIENT (KYC), POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO, AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (LDFT) E DE SUSTENTABILIDADE 20
8.1. Cadastro de clientes e atualização 22
8.2. Procedimentos relacionados às contrapartes 24
8.3. Pessoas Expostas Politicamente 25
8.4. Classificação de Risco e Monitoramento 26

8.5. Comunicações 30
8.6. Compromisso Socioambiental 32
9. ENVIO DE INFORMAÇÕES ÀS AUTORIDADES GOVERNAMENTAIS 34
10. PROCEDIMENTOS OPERACIONAIS 34
10.1. Registro de operações 35
10.2. Liquidação das Operações 35
11. POLÍTICA DE SELEÇÃO E CONTRATAÇÃO DE TERCEIROS 35
11.1. Objetivo 35
11.2. Definição 35
11.3. Aplicabilidade 36
11.4. Princípios de Aplicação e Normas de Conduta 36
11.5. Corretoras 36
11.6. Processo de Due Diligence 37
11.6.1. Identificação de potencial relação 38
11.6.2. Due diligence preliminar 38
11.6.3. Classificação quanto ao risco 38
11.6.4. Due diligence baseada em risco 39
11.6.5. Aprovação ou reprovação da contratação 40
11.6.6. Requisitos mínimos do contrato 41
11.7. Red Flags 41
11.8. Monitoramento 42
11.9. Violações e Sanções Aplicáveis 43
12. PLANO DE CONTINUIDADE DO NEGÓCIO 44
12.1. Estrutura e procedimentos de contingência 44
12.2. Plano de contingência 44
12.3. Atualização do plano de continuidade do negócio 45
13. SEGURANÇA CIBERNÉTICA 45
13.1. Avaliação dos riscos 45
13.2. Ações de prevenção e proteção 46

13.3. Monitoramento 47
13.4. Plano de resposta 48
13.5. Reciclagem e revisão 48
ANEXO I - Termo de Adesão 50
ANEXO II - Solicitação para Desempenho de Atividade Externa 52
ANEXO III – Classificação de Pessoa Exposta Politicamente 53

1. INTRODUÇÃO E OBJETIVO

O termo *compliance* é originário do verbo, em inglês, *to comply*, e significa "estar em conformidade com regras, normas e procedimentos".

Visto isso, as empresas do Grupo Onze ("Onze") adotaram em sua estrutura as atividades de "Controles Internos" ou "*Compliance*". O diretor responsável pelo *compliance* ("Diretor de *Compliance*") tem como objetivo garantir o cumprimento das leis e regulamentos emanados de autoridades competentes aplicáveis às atividades de Onze, bem como as políticas e manuais da Onze, e obrigações de fidúcia e lealdade devidas aos fundos de investimento e demais clientes cujas carteiras de títulos e valores mobiliários sejam geridas pela Onze ("Clientes"), prevenindo a ocorrência de violações, detectando as violações que ocorram e punindo ou corrigindo quaisquer de tais descumprimentos.

Este Manual de Controles Internos *(Compliance)* ("Manual de *Compliance*") foi elaborado para atender especificamente às atividades desempenhadas pela Onze, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de Compliance é aplicável a todos os sócios, diretores, funcionários, empregados, estagiários e demais colaboradores da Onze (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

Este Manual de Compliance deve ser lido em conjunto com o Código de Ética da Onze, que também contém regras que visam a atender aos objetivos aqui descritos.

Este Manual de Compliance está de acordo com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM").

2. PROCEDIMENTOS

2.1. Designação de um Diretor Responsável

A área de *compliance* é liderada pelo Diretor de *Compliance* devidamente nomeado no contrato social da Onze.

O Diretor de *Compliance* exerce suas funções com plena independência e não atua em funções que possam afetar sua isenção, dentro ou fora da Onze. Da mesma forma, a área de *compliance* não está sujeita a qualquer ingerência por parte da equipe de gestão e possui autonomia para questionar os riscos assumidos nas operações realizadas pela Onze.

O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance*, e caso tenha que se ausentar por um longo período de tempo, deverá ser substituído ou deverá designar um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada, caberá aos sócios da Onze fazê-lo.

O Diretor de *Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Onze no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Onze com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

São também atribuições do Diretor de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

(i) Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

(ii) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

(iii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética", assim como avaliar as demais situações que não foram previstas em todas as políticas internas da Onze ("Políticas Internas");

(iv) Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

(v) Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

(vi) Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

(vii) Reconhecer situações novas no cotidiano da administração interna ou nos negócios da Onze que não foram planejadas, fazendo a análise de tais situações;

(viii) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Onze; e

Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Onze, assim como das pessoas envolvidas no caso.

2.2. Revisão periódica e preparação de relatório

O Diretor de *Compliance* deverá revisar pelo menos anualmente este Manual de *Compliance* para verificar a adequação das políticas e procedimentos aqui previstos, e sua efetividade. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as violações ocorridas no período anterior, e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pela Onze.

2.3. Treinamento

A Onze possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre as Políticas Internas, inclusive este Manual de *Compliance,* aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

O Diretor de *Compliance* deverá organizar sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *compliance*.

A periodicidade mínima do processo de reciclagem continuada será anual. A cada processo de reciclagem continuada, os Colaboradores assinarão termo comprovando a participação no respectivo processo.

Os materiais, carga horária e grade horária serão definidos pelo Diretor de Compliance, que poderá, inclusive, contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

2.4. Apresentação do Manual de Compliance e suas modificações

O Diretor de *Compliance* deverá entregar uma cópia deste Manual de *Compliance*, e das Políticas Internas, para todos os Colaboradores por ocasião do início das atividades destes na Onze, e sempre que estes documentos forem modificados. Mediante o recebimento

deste Manual de *Compliance*, o Colaborador deverá confirmar que leu, entendeu e cumpre com os termos deste Manual de *Compliance* e das Políticas Internas, mediante assinatura do termo de adesão que deverá seguir o formato previsto no Anexo I ("Termo de Adesão").

2.5. Atividades Externas

Os Colaboradores devem obter a aprovação escrita do Diretor de *Compliance* antes de envolverem-se em negócios externos à Onze. "Atividades Externas" incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome da Onze ou não). Os Colaboradores que desejam ingressar ou engajar-se em tais Atividades Externas devem obter a aprovação prévia por escrito do Diretor de *Compliance* por meio da "Solicitação para Desempenho de Atividade Externa" na forma do Anexo II.

Não será necessária a prévia autorização do Diretor de *Compliance* para Atividades Externas relacionadas à caridade, organizações sem fins lucrativos, clubes ou associações civis.

2.6. Supervisão e responsabilidades

Todas as matérias de violações a obrigações de *compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas ao Diretor de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *compliance*, e determinar quais as sanções aplicáveis. O Diretor de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

2.7. Sanções

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de Compliance e/ou das Políticas Internas serão definidas e aplicadas pelo Diretor de Compliance, a seu critério razoável, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente, sem prejuízo da aplicação de penalidades pela CVM e do direito da Onze de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Instrução CVM nº 558, de 26 de março de 2015, especialmente o Artigo 24, III e Artigo 25, II, a Onze adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Onze é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

3.1. Segurança da Informação Confidencial

A Onze mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios de rede, planos de continuidade entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Onze, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da Onze, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento da Onze, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Onze.

Qualquer informação sobre a Onze, ou de qualquer natureza relativa às atividades da Onze, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Onze, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

Todos os Colaboradores, assim como todos os terceiros contratados pela Onze, deverão assinar documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Onze e circulem em ambientes externos à Onze com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Onze

e de seus Clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Onze.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, usando uma trituradora, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Onze.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Onze.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Onze, ou utilizar material, marca e logotipos da Onze para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

O Diretor de *Compliance* também monitorará e será avisado por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Diretor de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável

pela área de informática na Onze. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

A Onze se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Onze para a atividade profissional de cada Colaborador.

Todas as informações do servidor da Onze, do banco de dados dos clientes e os modelos dos analistas são enviados para servidor dedicado para armazenamento de longa duração no provedor de serviços em nuvem da Onze. Nesse servidor, as informações são segregadas por área e respeitando os acessos individuais de cada colaborador, sendo armazenadas com *backup*.

Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de *Compliance* apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

Em caso de vazamento, perda, furto ou roubo de quaisquer materiais ou equipamentos que contenham informações confidenciais, o Colaborador deverá notificar imediatamente o Diretor de *Compliance* sobre tal evento, por telefone, e-mail ou mensagem de texto.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Onze, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

3.2. Propriedade intelectual

Todos os documentos desenvolvidos na realização das atividades da Onze ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são de propriedade intelectual da Onze.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual da Onze fora do escopo de atuação ou não destinado aos Clientes, dependerá de prévia e expressa autorização por escrito do Diretor de *Compliance*.

Uma vez rompido com a Onze o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

4. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um Cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Onze que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pela Onze; *(b)* na decisão de Clientes de comprar, vender ou manter cotas de fundos de investimento administrados pela Onze; e *(c)* na decisão dos Clientes de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Onze.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso de o Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de *Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Onze, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao Diretor de *Compliance*.

4.1. Insider Trading, “Dicas” e Spoofing

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo a própria Onze e seus Colaboradores).

“Dica” é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

Spoofing corresponde, basicamente, à inserção de ofertas limitadas de compra (ou de venda) por diferentes preços, sem a intenção de executá-las, inserindo subsequentemente

oferta(s) de venda (ou de compra) do outro lado do livro que, após ser(em) executada(s), segue(m)-se da rápida remoção das ofertas limitadas inseridas inicialmente, criando, assim, possíveis condições artificiais de demanda.

A Onze não possui sistemas direcionados à prática de spoofing e, adicionalmente, deve monitorar todas as operações e ofertas realizadas, com o propósito de identificar, avaliar, registrar, coibir e comunicar o Diretor de *Compliance*, se necessário, das situações definidas na regulamentação vigente, notadamente nas Instruções CVM nº 8, de 08 de outubro de 1979 e nº 461/07, de 23 de outubro de 2007, respectivamente e conforme alteradas, como práticas abusivas, de criação de condições artificiais de demanda, oferta ou preço, manipulação de preços, operações fraudulentas, práticas não equitativas e *spoofing*.

É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Onze ou de terceiros.

A prática de qualquer ato em violação deste Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Instrução CVM nº 358, de 03 de janeiro de 2002 ("Instrução CVM 358").

É de responsabilidade do Diretor de *Compliance* verificar e processar periodicamente as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading*, "dicas" e *spoofing*. Casos envolvendo o uso de informação privilegiada, *insider trading*, "dicas" e *spoofing* devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com a Onze, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

5.1. Segregação física

Caso a Onze venha a desenvolver atividades que apresentem conflito de interesses com a atividade de gestão, a área de gestão de recursos da Onze será fisicamente segregada das demais, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas, para garantir que não exista circulação de informações que possam gerar conflito de interesses ("*chinese wall*").

Não será permitida a circulação de Colaboradores em seções que não sejam destinadas ao respectivo Colaborador.

Reuniões com terceiros não Colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não Colaborador, inclusive Clientes, sendo este encaminhado diretamente à devida sala.

É de competência do Diretor de *Compliance*, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções. Caso o Diretor de *Compliance* constate que o Colaborador tenha tentado acesso às áreas restritas com frequência acima do comum ou necessária, ou ainda sem qualquer motivo aparente, poderá aplicar as devidas sanções. Eventual infração à regra estabelecida neste Manual de *Compliance* será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Diretor de *Compliance*.

5.2. Segregação eletrônica

Adicionalmente, a Onze segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores, sendo que haverá impressora exclusivamente destinada à utilização da área de administração de recursos.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado, sendo certo que tal restrição/segregação será feita em relação a:

(i) cargo/nível hierárquico; e
(ii) equipe.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores

autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Onze permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

5.3. Especificidades dos mecanismos de controles internos

A Onze, por meio do Diretor de *Compliance*, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

(i) Definição de responsabilidades dentro da Onze;

(ii) Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;

(iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

(iv) Contínua avaliação dos diversos riscos associados às atividades da empresa; e

(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Onze estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de *Compliance*.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Onze, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

6. DIVULGAÇÃO DE MATERIAL DE MARKETING

Todos os Colaboradores devem ter ciência de que a divulgação de materiais de *marketing* deve ser realizada estritamente de acordo com as regras emitidas pela CVM e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e que não devem conter qualquer informação falsa ou que possa levar o público a erro.

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas à Onze, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão, que ofereça qualquer serviço de consultoria ou gestão prestado pela Onze, ou um produto de investimento da Onze no mercado de valores mobiliários (incluindo fundos geridos).

Quaisquer materiais de *marketing* devem ser previamente submetidos ao Diretor de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo, mas não se limitando à Instrução CVM nº 400, de 29 de dezembro de 2003 ("Instrução CVM 400"), a Instrução CVM nº 476, de 16 de janeiro de 2009 ("Instrução CVM 476"), a Instrução CVM nº 555, de 17 de dezembro de 2014 ("Instrução CVM 555"), o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, e diretrizes escritas emanadas da ANBIMA. O Diretor de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de *Compliance* é que qualquer material de *marketing* deve ser utilizado.

Abaixo encontra-se uma lista não exaustiva de regras aplicáveis a materiais de *marketing* de fundos de investimento.

Nos termos da Instrução CVM 555, qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

(i) ser consistente com o regulamento e com a lâmina, se houver;

(ii) ser elaborado em linguagem serena e moderada, advertindo seus leitores para os riscos do investimento;

(iii) ser identificado como material de divulgação;

(iv) mencionar a existência da lâmina, se houver, e do regulamento, bem como os endereços na rede mundial de computadores nos quais tais documentos podem ser obtidos;

(v) ser apresentado em conjunto com a lâmina, se houver;

(vi) conter as informações do item 12 do Anexo 42 da Instrução CVM 555, se a divulgação da lâmina não for obrigatória;

(vii) conter informações:

(a) verdadeiras, completas, consistentes e não induzir o Cliente a erro;
(b) escritas em linguagem simples, clara, objetiva e concisa;
(c) úteis à avaliação do investimento; e
(d) que não assegurem ou sugiram a existência de garantia de resultados futuros ou não isenção de risco para o Cliente.

Informações factuais devem vir acompanhadas da indicação de suas fontes e ser diferenciadas de interpretações, opiniões, projeções e estimativas.

Qualquer divulgação de informação sobre os resultados de fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses, a partir da data da primeira emissão de cotas.

Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente:

(i) mencionar a data do início de seu funcionamento;

(ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e a rentabilidade acumulada nos últimos 12 (doze) meses, não sendo obrigatória, neste caso, a discriminação mês a mês, ou no período decorrido desde a sua constituição, se inferior, observado que a divulgação de rentabilidade deve ser acompanhada de comparação, no mesmo período, com índice de mercado compatível com a política de investimento do fundo, se houver;

(iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde a sua constituição, se mais recente;

(iv) divulgar a taxa de administração e a taxa de performance, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e

(v) destacar o público-alvo do fundo e as restrições quanto à captação, de forma a ressaltar eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de investidores em geral.

Caso o administrador contrate os serviços de empresa de classificação de risco, deve apresentar, em todo o material de divulgação, o grau mais recente conferido ao fundo, bem como a indicação de como obter maiores informações sobre a avaliação efetuada.

Ficam incorporadas por referência, ainda, as disposições do Capítulo VI do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como das "Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento" da ANBIMA, disponíveis publicamente no *website* desta instituição.

7. APROVAÇÃO DE CORRETORAS E SOFT DOLLAR

A equipe de *compliance* manterá uma lista de corretoras aprovadas com base nos critérios estabelecidos pela Onze. O *trader* executará ordens exclusivamente com corretoras constantes na referida lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Diretor de *Compliance* atualizará a lista de corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

Os custos de transação mais relevantes tais como corretagem, emolumentos e custódia, devem ser constantemente monitorados, com o objetivo de serem minimizados. Anualmente, o time de gestão da Onze deve elaborar um *ranking* com critérios objetivos de corretoras levando em consideração qualidade do serviço e preço, visando encontrar a melhor equação e prezando o dever fiduciário que temos para com os nossos Investidores. A Onze somente utilizará as corretoras mais bem classificadas.

As equipes de gestão e de c*ompliance* devem rever o desempenho de cada corretora e considerar, entre outros aspectos: a qualidade das execuções fornecidas; o custo das execuções, acordos de *soft dollar* e potenciais conflitos de interesse.

7.1. Política de Soft Dollar

Quaisquer acordos envolvendo *soft dollars* devem ser previamente aprovados pelo Diretor de *Compliance*. *Soft dollars* podem ser definidos como quaisquer benefícios oferecidos por uma corretora a uma gestora que direcione ordens para a corretora, que podem incluir, sem limitação, *researches* e acesso a sistemas de informações de mercado como o *Bloomberg*.

Acordos de *soft dollar* somente poderão ser aceitos pelo Diretor de *Compliance* se quaisquer benefícios oferecidos (i) possam ser utilizados diretamente para melhorias da tomada de decisão de investimento pela Onze; (ii) sejam razoáveis em relação ao valor das comissões pagas; e (iii) não afetem a independência da Onze.

A prática de *soft dollar* é aceita única e exclusivamente para as atividades diretamente relacionadas à gestão dos recursos dos Clientes.

Os acordos de *soft dollars* não criam nenhuma obrigação para a Onze operar exclusivamente junto às corretoras que concedem os benefícios.

Atualmente, a Onze não possui qualquer acordo de *soft dollar.*

8. POLÍTICA DE KNOW YOUR CLIENT (KYC), POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO, AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (LDFT) E DE SUSTENTABILIDADE

O termo “lavagem de dinheiro” abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. A Onze e seus Colaboradores devem obedecer a todas as regras de prevenção à lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613, de 03 de março de 1998, conforme alterada (“Lei 9.613/98”), e a Resolução CVM nº 50, de 02 de setembro de 2021 (“Resolução CVM 50”), cujos principais termos estão refletidos neste Manual de *Compliance*.

O Diretor de *Compliance* será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro.

O Diretor de *Compliance* estabelecerá o devido treinamento dos Colaboradores da Onze – na forma deste Manual de *Compliance* – para que estes estejam aptos a reconhecer e a combater a lavagem de dinheiro, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

A Onze adota os seguintes procedimentos permanentes de controle e vigilância, visando minimizar o risco de ocorrência de lavagem de dinheiro nas diversas operações financeiras sob sua responsabilidade, a saber:

(i) Análise, pela área de Compliance, das movimentações financeiras que possam indicar a existência de crime, em razão de suas características, valores, formas de realização e instrumentos utilizados, ou que não apresentem fundamento econômico ou legal;

(ii) Evitar realizar qualquer operação comercial ou financeira por conta de terceiros, a não ser que seja transparente, justificada e sólida, além de viabilizada ou executada através de canais bancários;

(iii) Evitar operações com pessoas ou entidades que não possam comprovar a origem do dinheiro envolvido;

(iv) Evitar operações financeiras internacionais complexas, que envolvam muitas movimentações de dinheiro em países diferentes e/ou entre bancos diferentes;

(v) Avaliação das políticas e práticas de prevenção e combate à lavagem de dinheiro adotada por terceiros/parceiros da Onze;

(vi) Certificar-se de que os distribuidores das cotas dos fundos de investimento geridos pela Onze realizaram os procedimentos para verificação da adequação do perfil dos Clientes aos fundos de investimento geridos pela Onze nos quais esses Clientes invistam;

(vii) Registro e guarda das informações relativas às operações e serviços financeiros dos Clientes;

(viii) Comunicação ao Conselho de Controle de Atividades Financeiras (“COAF”) e à CVM, no prazo legal, de propostas e/ou operações consideradas suspeitas ou atípicas, a menos que não seja objetivamente permitido fazê-lo;

(ix) Comunicação ao COAF e à CVM de operações em espécie, ou cujo montante atinja os patamares fixados pelos reguladores;

(x) Revisão periódica dos procedimentos e controles de prevenção e combate à lavagem de dinheiro e de controles internos;

(xi) Adoção de procedimento de especial atenção a PPE, conforme definido abaixo; e

(xii) Ter adequado conhecimento dos Colaboradores e fazê-los conhecer políticas e normativos aderentes aos órgãos reguladores.

A Onze adota procedimentos que permitem o monitoramento das faixas de preços das cotas de fundos geridos, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas, e se for o caso, comunicados aos órgãos competentes.

8.1. Cadastro de clientes e atualização

Nos termos da Resolução CVM 50, o cadastro dos Clientes da Onze deve abranger, no mínimo, as informações e documentos indicados abaixo:

(i) Pessoa física: (a) nome completo, sexo, profissão, data de nascimento, naturalidade, nacionalidade, estado civil, filiação, nome do cônjuge ou companheiro; (b) natureza e número do documento de identificação, nome do órgão expedidor e data de expedição; (c) número de inscrição no Cadastro de Pessoas Físicas ("CPF/MF"); (d) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP) e número de telefone; (e) endereço eletrônico para correspondência; (f) ocupação profissional e entidade para a qual trabalha; (g) informações sobre os rendimentos e a situação patrimonial; (h) informações sobre perfil de risco e conhecimento financeiro do Cliente; (i) se o Cliente autoriza ou não a transmissão de ordem por procurador; (j) a indicação de se há procuradores ou não; (k) qualificação dos procuradores e descrição de seus poderes, se houver; (l) datas das atualizações do cadastro; (m) assinatura do Cliente; (n) cópia dos seguintes documentos: documento de identidade e comprovante de residência ou domicílio; e (o) cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(ii) Pessoa jurídica: (a) a denominação ou razão social; (b) nomes e CPF/MF dos controladores diretos ou razão social e inscrição no Cadastro Nacional de Pessoa Jurídica ("CNPJ") dos controladores diretos; (c) nomes e CPF/MF dos administradores; (d) nomes dos procuradores; (e) número de CNPJ e NIRE; (f) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP); (g) número de telefone; (h) endereço eletrônico para correspondência; (i) atividade principal desenvolvida; (j) faturamento médio mensal dos últimos doze meses e a situação patrimonial; (k) informações sobre perfil de risco e conhecimento financeiro do Cliente; (l) denominação ou razão

social de pessoas jurídicas controladoras, controladas ou coligadas; (m) se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas; (n) se o Cliente autoriza ou não a transmissão de ordens por representante ou procurador; (o) qualificação dos representantes ou procuradores e descrição de seus poderes; (p) datas das atualizações do cadastro; (q) assinatura do Cliente; (r) cópia dos seguintes documentos: CNPJ, documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente, e atos societários que indiquem os administradores da pessoa jurídica, se for o caso; e (s) cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(iii) Demais hipóteses: (a) a identificação completa dos Clientes; (b) a identificação completa de seus representantes e/ou administradores; (c) situação financeira e patrimonial; (d) informações sobre perfil de risco e conhecimento financeiro do Cliente; (e) se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas; (f) datas das atualizações do cadastro; e (g) assinatura do Cliente.

Em caso de Clientes não residentes no país, o cadastro deve, adicionalmente, conter: *(i)* os nomes das pessoas naturais autorizadas a emitir ordens e, conforme o caso, dos administradores da instituição ou responsáveis pela administração da carteira; e *(ii)* os nomes do representante legal e do responsável pela custódia dos seus valores mobiliários. Ainda, a Onze adotará procedimentos para identificação da pessoa natural caracterizada como beneficiário final, nos termos da legislação e regulamentação vigentes.

As alterações ao endereço constante do cadastro dependem de ordem do Cliente, escrita ou por meio eletrônico, e comprovante do correspondente endereço.

Do cadastro deve constar declaração, datada e assinada pelo Cliente ou, se for o caso, por procurador legalmente constituído, de que (conforme aplicável):

(i) são verdadeiras as informações fornecidas para o preenchimento do cadastro;

(ii) o Cliente se compromete a informar, no prazo de 10 (dez) dias, quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, inclusive eventual revogação de mandato, caso exista procurador;

(iii) o Cliente é pessoa vinculada ao intermediário, se for o caso;

(iv) o Cliente não está impedido de operar no mercado de valores mobiliários;

(v) suas ordens devem ser transmitidas por escrito, por sistemas eletrônicos de conexões automatizadas ou telefone e outros sistemas de transmissão de voz; e

(vi) o Cliente autoriza os intermediários, caso existam débitos pendentes em seu nome, a liquidar os contratos, direitos e ativos adquiridos por sua conta e ordem, bem como a executar bens e direitos dados em garantia de suas operações ou que estejam em poder do intermediário, aplicando o produto da venda no pagamento dos débitos pendentes, independentemente de notificação judicial ou extrajudicial.

A critério exclusivo da Onze, nos casos em que entender necessário, poderão ser requeridas, adicionalmente à documentação e informações previstas acima, visitas *due diligence* na residência, local de trabalho ou instalações comerciais do Cliente.

Após a análise e verificação, pela área de *Compliance*, dos documentos e informações fornecidos pelo Cliente, a área de C*ompliance* decidirá pela aprovação ou recusa do cadastro do Cliente. O fornecimento da totalidade dos documentos e informações solicitados não é garantia da aprovação do cadastro do Cliente, podendo a Onze recusar o cadastramento de Clientes a seu exclusivo critério.

O cadastro de cada cliente ativo (assim entendido aquele que tenha efetuado movimentações ou apresente saldo no período de 24 (vinte e quatro) meses posteriores à última atualização), deve ser atualizado em intervalos não superiores a 36 (trinta e seis) meses, conforme a sua classificação de risco.

O processo de atualização deve ser evidenciado por meio de fichas cadastrais e/ou cartas assinadas pelos Clientes, *logs* de sistemas, gravações telefônicas, entre outros comprovantes de confirmação de dados. Nenhuma operação deve ser realizada para a carteira de Clientes cujo cadastro esteja incompleto.

Quaisquer dúvidas relativas a cadastro e suas atualizações devem ser submetidas ao Diretor de *Compliance*.

8.2. Procedimentos relacionados às contrapartes

A Onze é responsável por tomar todas as medidas necessárias, segundo a legislação e regulamentação aplicável, incluindo, mas não limitado a, Lei 9.613/98 e Resolução CVM 50 as regras de cadastro, *know your client* - KYC (“conheça seu cliente”), *know your employee* – KYE (“conheça seu funcionário”) e *know your partner* – KYP (“conheça seu parceiro”) presentes neste Manual de Compliance e as melhores práticas adotadas pelas entidades autorreguladoras do mercado, para estabelecer e documentar a verdadeira e completa

identidade, situação financeira e o histórico de cada contraparte nas operações realizadas pelos fundos de investimento.

Nesse sentido, além dos clientes de suas carteiras, a Onze busca analisar e monitorar, para fins de cumprimento às normas de prevenção à lavagem de dinheiro, as contrapartes com quem venha negociar os ativos que pretende adquirir, visando uma eficaz prevenção de quaisquer atividades inidôneas em seus ativos sob gestão.

8.3. Pessoas Expostas Politicamente

Os procedimentos para a identificação e negociação com pessoas expostas politicamente ("PEP") são tratados na Resolução CVM 50 e na Lei nº 9.613/98, e alterações posteriores, e demais normas editadas pelo BACEN, Conselho Monetário Nacional e GAFI/FATF.

A definição de PEP consta no Artigo 1º-B do Anexo A da Resolução CVM 50, também replicado no Anexo III desse Manual.

Além disso, Circular do BACEN nº 3.461, de 24 de julho de 2009, e alterações posteriores, dispõe sobre os procedimentos a serem observados pelos agentes financeiros para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PEP, os quais devem ser estruturados de forma a possibilitar a caracterização de pessoas consideradas PEP e identificar a origem dos fundos envolvidos nas transações dos Clientes assim identificados.

Recomenda-se aos sujeitos obrigados a especial, reforçada e contínua atenção no exame e cumprimento das medidas preventivas, sobretudo no que se refere às relações jurídicas mantidas com PEP, nos seguintes termos:

(i) Supervisão de maneira mais rigorosa a relação de negócio mantido com PEP;

(ii) Dedicação de especial atenção a propostas de início de relacionamento e a operações executadas com PEP, inclusive as oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política;

(iii) Manutenção de regras, procedimentos e controles internos para identificação de Clientes que se tornaram após o início do relacionamento com a instituição ou que seja constatado que já eram PEP no início do relacionamento com a instituição e aplicar o mesmo tratamento dos itens acima; e

(iv) Manutenção de regras, procedimentos e controles internos para identificação da origem dos recursos envolvidos nas transações dos Clientes e dos beneficiários identificados como PEP.

Adicionalmente, recomenda-se a observação de outros fatores de risco, antes da aprovação de uma conta de PEP:

(i) Transparência da fonte do dinheiro e dos bens para assegurar que estes não resultaram de recursos do Estado;

(ii) Avaliação se a finalidade da conta e o nível de atividade proposto estão de acordo com o perfil financeiro geral da pessoa;

(iii) Cargo político atual ou anteriormente exercido e sua duração;

(iv) O nível de acesso da PEP a fundos estatais;

(v) Avaliação da transparência e da complexidade da estrutura e da posse da conta; e

(vi) O regime político e socioeconômico do país de origem, seu nível de corrupção e controle de drogas.

8.4. Classificação de Risco e Monitoramento

Nos termos da Resolução CVM 50, a Onze, no limite de suas atribuições, identifica, analisa, compreende e mitiga os riscos de LDFT inerentes às suas atividades desempenhadas no mercado de valores mobiliários, adotando uma abordagem baseada em risco (“ABR”) para garantir que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados e assegurando o cumprimento da referida instrução e das demais disposições e diretrizes regulatórias e autorregulatórias de PLDFT.

Desta forma, a Onze classifica em baixo, médio e alto risco de LDFT os serviços prestados, produtos oferecidos, canais de distribuição, seus clientes e prestadores de serviço.

A Onze, por meio da área de Compliance e da Diretora de PLD, monitorará a adequação dos critérios utilizados nesta Política para a definição e classificação da sua ABR, a partir (i) do acompanhamento constante da regulamentação e autorregulação, (ii) dos testes de aderência e índices de efetividade, (iii) da avaliação do impacto às definições aqui previstas em razão de eventuais novos serviços prestados, produtos oferecidos, canais de

distribuição, clientes, prestadores de serviços, agentes envolvidos nas operações, e novos ambientes de negociação e registro, bem como (iv) da avaliação do impacto de rotinas da Onze relacionadas aos deveres de observância de outros normativos, tais como em relação ao normativo que trata sobre condições artificiais de demanda, oferta ou preço de valores mobiliários, manipulação de preço, operações fraudulentas e práticas não equitativas.

8.4.1. Classificação de Risco

Especificamente sobre os clientes, a Onze adota a abordagem definida abaixo:

a) Alto Risco – clientes que apresentem pelo menos uma das seguintes características:

- Acusados e condenados em processo judicial relativo a práticas de LDFT nos últimos 5 (cinco) anos ou em processos que sejam considerados graves pelo Diretor de PLD;
- Em relação aos quais existam notícias desabonadoras na mídia que tenham relevância para fins de LDFT;
- Sejam Pessoa Exposta Politicamente, nos termos da Resolução CVM 50
- Que se recusem a fornecer as informações necessárias ou apresentem informações cadastrais com consideráveis inconsistências, incluindo, mas não se limitando aos que investem valores incompatíveis com a ocupação profissional e a situação financeira patrimonial declarada;
- Que não apresentem informações e documentos necessários que permitam a identificação do beneficiário final pela Onze, conforme aplicável e ressalvadas as exceções previstas na regulamentação em vigor, incluindo os casos de INR que sejam (v.1) entes constituídos sob a forma de *trusts* ou outros veículos fiduciários; (v.2) sociedades constituídas com títulos ao portador, e (v.3) pessoas físicas residentes no exterior;
- Que sejam pessoas naturais, jurídicas ou outras entidades que residam, tenham sede ou sejam constituídas em ou, ainda, cujos recursos investidos sejam provenientes de jurisdição offshore que: (vi.1) seja classificada por organismos internacionais, em especial o GAFI, como não cooperante ou com deficiências estratégicas, em relação à prevenção e ao combate à lavagem de dinheiro e ao financiamento do terrorismo; (vi.2) faça parte de lista de sanções ou restrições emanadas pelo CSNU, bem como de eventuais outras listas de monitoramento obrigatório, nos termos da regulamentação em vigor; e (vi.3) não possua órgão regulador do mercado de capitais, em especial, que tenha celebrado com a CVM acordo de cooperação mútua que permita o intercâmbio de informações financeiras

de investidores, ou seja signatário do memorando multilateral de entendimento da Organização Internacional das Comissões de Valores – OICV/IOSCO;
- Que sejam organização sem fins lucrativos, nos termos da legislação específica;
- Que realizem ameaça a Colaborador da Onze, direta ou indiretamente, tentando dissuadi-lo de registrar os relatórios necessários ou cumprir com qualquer norma, orientação ou diretriz de regulação, autorregulação e interna da Onze; ou
- Que desistam de proceder com alguma operação apenas depois de descobrir que esta ou algum elemento desta deverá ser comunicado, registrado ou de qualquer forma reportado para fins regulatórios.

b) Médio Risco – clientes que, embora não existam inconsistências relevantes em seu cadastro, não tenham fornecido documentação cadastral integral ou que, ainda que a tenham fornecido, não haja plena clareza das informações ali constantes.

c) Baixo Risco – clientes que não se enquadram nas definições acima.

8.4.2. Monitoramento

As situações listadas abaixo podem configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613, ou podem com eles relacionar-se, devendo a Onze acompanhar a evolução do seu relacionamento com o cliente e atribuir maior atenção a tais situações para fins de manutenção e/ou alteração da classificação de ABR a ele atribuída, bem como quanto à necessidade de providências adicionais junto às autoridades competentes:

- Atividades com indícios de atipicidade de que tenha conhecimento;
- Transações que violam os programas de sanções econômicas;
- Transações com volumes e valores significativos e incompatíveis com a ocupação profissional, os rendimentos ou a situação patrimonial ou financeira declarada do Cliente Direto, ou destoantes dos historicamente efetuados;
- Transações com volumes e valores significativos e incompatíveis com a atividade econômica, objeto social ou do faturamento informado pelo Cliente Direto, no caso de pessoa jurídica, com o padrão operacional apresentado por clientes com o mesmo perfil;
- Eventuais reincidências do desenquadramento de perfil histórico de transações, observado o parágrafo abaixo;
- Clientes em relação aos quais existam notícias desabonadoras na mídia que tenham relevância para fins de LDFT;

- Situações em que o Cliente Direto apresente aparente propósito oculto ou comportamento não usual na solicitação da operação;
- Clientes que realizem ameaça a Colaborador da Onze, direta ou indiretamente, tentando dissuadi-lo de registrar os relatórios necessários ou cumprir com qualquer norma, orientação ou diretriz de regulação, autorregulação e interna da Onze;
- Operações cujas características e desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- Operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelos clientes;
- Situações em que não seja possível identificar os beneficiários finais dos clientes;
- Situações em que não seja possível manter atualizada as informações cadastrais dos clientes;
- Clientes pessoas naturais, jurídicas ou outras entidades que residam, tenham sede ou sejam constituídas em ou, ainda, cujos recursos investidos sejam provenientes de jurisdição offshore que: (i) seja classificada por organismos internacionais, em especial o GAFI, como não cooperante ou com deficiências estratégicas, em relação à prevenção e ao combate à lavagem de dinheiro e ao financiamento do terrorismo; (ii) com tributação favorecida e submetidos a regimes fiscais privilegiados, conforme normas emanadas pela Receita Federal do Brasil; (iii) não possua órgão regulador do mercado de capitais, em especial, que tenha celebrado com a CVM acordo de cooperação mútua que permita o intercâmbio de informações financeiras de investidores, ou seja signatário do memorando multilateral de entendimento da OICV/IOSCO;
- Ameaça a Colaboradores, tentando dissuadi-lo de registrar os relatórios necessários;
- Negativa do Cliente Direto em continuar com uma transação depois de descobrir que ela precisa ser relatada;
- Sugestão por parte do Cliente Direto de pagamento de gratificação a Colaboradores; e
- Clientes que desempenhem atividade em que seja possível circular dinheiro em espécie e que a contabilidade possa ser mais facilmente alterada.

Adicionalmente ao monitoramento das operações e situações acima, a Onze realiza a atualização cadastral de acordo com o cronograma abaixo indicado, conforme grau de risco atribuído ao cliente:

a) Alto Risco: a cada 12 (doze) meses a Onze deverá realizar a atualização cadastral destes clientes. A área de Compliance destinará especial atenção para aqueles clientes classificados como de Alto Risco, devendo monitorar continuamente e de

maneira diferenciada a relação de negócio e as propostas de início de relacionamento.

b) Médio Risco: a cada 24 (vinte e quatro) meses a Onze deverá realizar a atualização cadastral destes clientes.

c) Baixo Risco: a cada 36 (trinta e seis) meses a Onze deverá realizar a atualização cadastral destes clientes.

8.5. Comunicações

Se algum Colaborador perceber ou suspeitar da prática de atos relacionados à lavagem de dinheiro ou outras atividades ilegais por parte de qualquer Cliente, este deverá imediatamente reportar suas suspeitas ao Diretor de *Compliance*, que deverá, então, instituir investigações adicionais, para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão. Entre outras possibilidades, uma atividade pode ser considerada suspeita se:

(i) operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;

(ii) operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;

(iii) operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;

(iv) operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

(v) operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

(vi) operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);

(vii) operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

(viii) operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;

(ix) operações liquidadas em espécie, se e quando permitido;

(x) transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;

(xi) operações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do Cliente ou de seu representante;

(xii) depósitos ou transferências realizadas por terceiros, para a liquidação de operações de Cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;

(xiii) pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do Cliente;

(xiv) situações em que não seja possível manter atualizadas as informações cadastrais de seus Clientes;

(xv) situações e operações em que não seja possível identificar o beneficiário final; e

(xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas.

A Onze deverá dispensar especial atenção às operações em que participem as seguintes categorias de Clientes:

(i) clientes não-residentes, especialmente quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador;

(ii) clientes com grandes fortunas geridas por áreas de instituições financeiras voltadas para clientes com este perfil (*private banking*); e

(iii) pessoas politicamente expostas.

A Onze deverá analisar as operações em conjunto com outras operações conexas e que possam fazer parte de um mesmo grupo de operações ou guardar qualquer tipo de relação entre si.

Os Colaboradores não devem divulgar suas suspeitas ou descobertas em relação a qualquer atividade, para pessoas que não sejam o Diretor de *Compliance*. Qualquer contato entre a Onze e a autoridade relevante sobre atividades suspeitas deve ser feita somente pelo Diretor de *Compliance*. Os Colaboradores devem cooperar com o Diretor de *Compliance* durante a investigação de quaisquer atividades suspeitas.

A Onze deve manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que a Onze previna qualquer danificação, falsificação, destruição ou alteração indevida dos livros e registros por meio de adoção de métodos necessários e prudentes.

Consideram-se operações relacionadas com terrorismo ou seu financiamento aquelas executadas por pessoas que praticam ou planejam praticar atos terroristas, que neles participam ou facilitam sua prática, bem como por entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas e as pessoas ou entidades que atuem sob seu comando.

8.6. Compromisso Socioambiental

A Onze reconhece a importância da sustentabilidade e responsabilidade socioambiental em todas as suas operações. Por esta razão, comprometemo-nos a promover práticas que visam a preservação do meio ambiente, o bem-estar da comunidade e o desenvolvimento sustentável. O nosso compromisso socioambiental baseia-se nos seguintes princípios:

- Preservação Ambiental: Comprometemo-nos a adotar medidas para minimizar nosso impacto ambiental, gerenciar resíduos de forma responsável, promover o uso eficiente de recursos naturais e implementar práticas sustentáveis em nossas operações.

- Respeito à Comunidade: Valorizamos as comunidades locais em que operamos e buscamos contribuir positivamente para o seu desenvolvimento. Comprometemo-nos a estabelecer relações de respeito, transparência e diálogo com as partes interessadas, buscando sempre o benefício mútuo.

- Ética e Integridade: Pautamos nossas ações em princípios éticos e de integridade, agindo de forma responsável e transparente em todas as nossas atividades. Repudiamos práticas que violem direitos humanos, trabalhistas e ambientais.

- Melhoria Contínua: Comprometemo-nos com a melhoria contínua de nossas práticas socioambientais, por meio da definição de objetivos e metas, monitoramento de desempenho e engajamento das partes interessadas.

- Conformidade Legal: Comprometemo-nos a cumprir integralmente a legislação ambiental e trabalhista aplicável, bem como os padrões de sustentabilidade e responsabilidade corporativa.

A Onze implementa estratégias sustentáveis em diferentes setores, visando a diminuição de seu impacto ambiental e a contribuição positiva para a sociedade, conforme exemplificado a seguir:

I. Reciclagem: A Onze adota programas abrangentes de reciclagem de resíduos sólidos em suas instalações corporativas. Contamos com lixeiras estrategicamente posicionadas e devidamente identificadas para a separação eficiente de materiais, garantindo assim sua destinação correta para processos de reciclagem e contribuindo ativamente para a redução do impacto ambiental.

II. Uso de Recursos Naturais: Comprometemo-nos a implementar e promover medidas destinadas a minimizar o consumo de recursos naturais essenciais, como água e plástico. Além disso, incentivamos práticas de conservação, como a conscientização dos colaboradores para evitar o desperdício de água e a utilização exclusiva de utensílios reutilizáveis, como os copos de vidro ou biodegradáveis, visando a preservação dos recursos naturais.

III. Filantropia e Doações: A Onze mantém o compromisso com a responsabilidade social e o engajamento comunitário. Através de iniciativas de filantropia e doações estruturadas, como a campanha do agasalho, apoiamos ativamente comunidades

locais e instituições de caridade, visando contribuir de maneira efetiva para o bem-estar social e o desenvolvimento sustentável das regiões em que atuamos.

9. ENVIO DE INFORMAÇÕES ÀS AUTORIDADES GOVERNAMENTAIS

As leis e regulamentações brasileiras exigem que o gestor de investimentos entregue informações periódicas e/ou informações eventuais relacionadas à sua atividade de gestão de ativos nos mercados de capitais do Brasil. Algumas destas informações serão apresentadas à CVM ou ANBIMA e outros serão apresentados às companhias em que os fundos de investimento (ou outro veículo de investimento) investem ou aos cotistas desses fundos de investimento.

Estas informações incluem, sem limitação, (i) as comunicações previstas na Instrução CVM 358, sobre posições detidas nas companhias que integram as carteiras dos veículos de investimento, nos termos ali especificados; (ii) atualização anual do formulário de referência, conforme exigido pelo artigo 15 da Instrução CVM 558, o qual contém, sem limitação, informações sobre os fundos geridos, valores sob gestão e tipos de investidores; (iii) revisão periódica de seus manuais, códigos e políticas, os quais devem ser disponibilizados no website da Onze; e (iv) informações exigidas pela legislação e regulamentação que trata da prevenção à lavagem de dinheiro.

O Anexo III contém uma lista não exaustiva das informações periódicas exigidas pela legislação e pela regulamentação da CVM e ANBIMA na data deste Manual de *Compliance*.

10. PROCEDIMENTOS OPERACIONAIS

A Onze atua em conformidade com os padrões e valores éticos elevados, principalmente observando e respeitando as normas expedidas pelos órgãos reguladores e suas Políticas Internas. Na condução de suas operações, a Onze deverá:

(i) observar o princípio da probidade na condução de suas atividades;

(ii) prezar pela capacitação para o desempenho das atividades;

(iii) agir com diligência no cumprimento das ordens, observado o critério de divisão das ordens (quando for o caso);

(iv) obter e apresentar aos seus clientes informações necessárias para o cumprimento das ordens;

(v) adotar providências para evitar a realização de operações em situação de conflito de interesses, assegurando tratamento equitativo a seus clientes; e

(vi) manter, sempre, os documentos comprobatórios das operações disponíveis, tanto para os órgãos fiscalizadores, como para os investidores e clientes, pelos prazos legais.

10.1. Registro de operações

As operações serão registradas nos sistemas dos administradores fiduciários dos fundos de investimento cujas carteiras sejam geridas pela Onze e no sistema da Onze com o intuito de controlar e conferir as carteiras disponibilizadas por estes administradores.

10.2. Liquidação das Operações

As operações serão liquidadas pelos próprios fundos de investimentos, obedecidos os critérios estabelecidos pelos administradores fiduciários e instituições financeiras onde as operações foram realizadas.

11. POLÍTICA DE SELEÇÃO E CONTRATAÇÃO DE TERCEIROS

11.1. Objetivo

Esta Política trata sobre as diretrizes para as contratações de terceiros e é pautada nas boas práticas comerciais e de gestão, sendo um complemento às normas e políticas internas da Onze, inclusive o Código de Ética e Manual de Controles Internos.

Esta Política é elaborada em conformidade com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como demais normas regulatórias e autorregulatórias aplicáveis.

11.2. Definição

Para os fins da presente Política, considera-se terceiro qualquer pessoa natural, empresa individual (pessoa jurídica) ou sociedade empresária (sociedade anônima, limitada, etc.) que comercialize e forneça produtos e materiais, ou que preste serviço de qualquer natureza diretamente à Onze ou aos seus clientes, sendo aplicável também a eventuais subcontratados (em conjunto “Terceiros”, indistintamente e, individualmente "Terceiro").

11.3. Aplicabilidade

Os processos aqui descritos se aplicam a todas as seleções e contratações de Terceiros pela Onze devem ser direcionados para assegurar que os respectivos contratos sigam os requisitos aqui estabelecidos.

As normas aqui contidas se aplicam a todos os sócios, administradores, empregados, funcionários, *trainees* e estagiários da Onze (em conjunto os "Colaboradores" e, individualmente, o "Colaborador").

11.4. Princípios de Aplicação e Normas de Conduta

Os seguintes princípios devem orientar a implementação dos procedimentos previstos nesta Política:

1) Risco: as análises e procedimentos de *due diligence* descritos nesta Política representam um processo de identificação, avaliação e tentativa de atenuação de risco. Não existe um processo que possa proteger completamente a Onze de riscos decorrentes da contratação de Terceiros. O objetivo deve ser avaliar amplamente estas ações e abordar os aspectos que parecem apresentar um risco material para a Onze.

2) Flexibilidade: embora esta Política estabeleça determinadas regras, procedimentos e fatores de risco, elas não podem ser aplicadas indiscriminadamente, devendo seguir um enfoque com base no risco. A identificação, avaliação e atenuação de riscos deve ser realizada de forma suficientemente flexível para se adaptar às realidades enfrentadas pela Onze e as especificidades de cada contratação. O Diretor de *Compliance* tem flexibilidade para aplicar os procedimentos de *due diligence* com base em seus critérios e avaliações de risco. Caso uma situação particular apresente um risco adicional, os Colaboradores devem consultar o Diretor de *Compliance*.

3) Monitoria contínua: o processo de monitoria e supervisão dos Terceiros é constante e continua mesmo após o término do processo formal de *due diligence* e a contratação do Terceiro.

11.5. Corretoras

Na seleção de corretoras, a Onze deverá realizar análise criteriosa e objetiva dos aspectos qualitativos da empresa, buscando o melhor interesse para os investidores.

Devem ser avaliadas, principalmente, as questões societárias, o histórico da instituição e dos sócios e diretores, capacidade operacional e de execução e o custo.

Serão levadas em consideração as taxas de corretagem, devolução e os serviços apresentados. Adicionalmente, a Onze poderá exigir o fornecimento de documentos que comprovem a qualificação técnica da corretora, além de outros documentos que a Área de *Compliance* entenda serem pertinentes para a avaliação.

O Diretor de *Compliance* manterá uma lista de corretoras aprovadas com base nos critérios estabelecidos pela Onze. O *trader* executará ordens exclusivamente com corretoras constantes referida lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Diretor de *Compliance* atualizará a lista de corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

A equipe de gestão e o Diretor de *Compliance* devem rever o desempenho de cada corretora e considerar, entre outros aspectos, a qualidade e o custo das execuções, acordos de *soft dollar* e potenciais conflitos de interesse.

Os acordos de *soft dollar* firmados pela Onze estarão disponíveis aos seus clientes mediante solicitação prévia, a qual poderá ser feita pelo endereço eletrônico: juridico@onze.com.br.

11.6. Processo de Due Diligence

Buscando mitigar o risco na contratação de Terceiros, a Onze realiza processo de *due diligence* junto a todos os Terceiros, por meio do qual analisa informações sobre a qualificação técnica, reputação e demais dados relevantes do Terceiro.

Além disso, o nível de diligência a ser adotado pela Onze em relação a cada Terceiro varia em função dos riscos associados à respectiva contratação, os quais são determinados considerando o tipo de Terceiro envolvido, os serviços a serem prestados, o alcance e o custo do contrato e a identificação de qualquer *red flag* (conforme item 11.7 desta Política).

Para tal fim, a Onze deve reunir e arquivar informação suficiente para avaliar os riscos associados a cada Terceiro, incluindo, no mínimo:

a) Uma descrição da justificativa comercial da contratação;
b) As qualificações e a reputação do Terceiro;
c) As relações do Terceiro com agentes públicos, como, por exemplo, a participação de agente público no capital social do Terceiro, a publicidade de tal relação etc.; e
d) A razoabilidade da remuneração proposta ao Terceiro.

Em relação à alínea “d” acima, a Onze poderá aplicar requisitos adicionais em relação ao processo de seleção, como o estabelecimento de número mínimo de propostas ou cotações.

Caberá aos membros da Área de *Compliance* verificar e documentar cada etapa do processo de *due diligence* dos Terceiros, as quais são detalhadas abaixo.

11.6.1. Identificação de potencial relação

Ao identificar a possível relação com um Terceiro, o membro da Área de *Compliance* responsável deverá preencher um formulário de justificativa da respectiva relação comercial ("Formulário de Justificativa"), incluindo informações básicas sobre o Terceiro e a relação proposta, no intuito de avaliar a adequação da relação e da remuneração proposta.

O membro da Área de *Compliance* responsável, então, iniciará o processo de *due diligence* do Terceiro, através do encaminhamento do Formulário de Justificativa ao Diretor de *Compliance*.

11.6.2. Due diligence preliminar

Após os procedimentos acima, o Diretor de *Compliance* deverá:

(i) Revisar as informações do Terceiro fornecidas no Formulário de Justificativa;

(ii) Avaliar se há, contra o Terceiro e/ou seus sócios e diretores, sanções aplicadas pelas autoridades governamentais pertinentes e/o se o Terceiro e/ou seus sócios e diretores constam em listas de restrições de órgãos como a Organização das Nações Unidas – ONU, *Office of Foreign Assets Control* – OFAC etc;

(iii) Questionar ao Terceiro se algum de seus sócios, diretores, funcionários ou colaboradores a qualquer título, ou qualquer pessoa a eles vinculada, exerce função pública; e

(iv) Realizar e documentar uma busca *online* em relação ao Terceiro, seus sócios e diretores, registrando qualquer elemento ou informação que possa suscitar dúvidas em relação à reputação do Terceiro, ou que indique a existência de relação entre o Terceiro, seus sócios ou seus diretores, com agentes públicos.

11.6.3. Classificação quanto ao risco

A partir das informações obtidas através da busca prevista na alínea "iv" do item 11.6.2 acima, os membros da Área de *Compliance* deverão realizar uma avaliação preliminar de cada Terceiro, no intuito de atribuir o nível de risco a ele associado, que poderá ser "baixo",

“médio” ou “alto”. A partir do nível de risco atribuído, a Área de *Compliance* determinará o nível da diligência a ser empregada na avaliação e supervisão do Terceiro, conforme os procedimentos descritos no item 11.6.4 e 11.7 abaixo.

A Onze aplicará os seguintes critérios para classificação do Terceiro conforme o nível de risco a ele associado, sem limitação:

a) Tipo de serviço a ser prestado pelo Terceiro;
b) Valor da remuneração proposta;
c) Existência de relações conhecidas do Terceiro e/ou de seus sócios e diretores com órgãos e/ou agências governamentais, empresas públicas e/ou agentes públicos;
d) Verificação de *red flags*, conforme item 7 abaixo;
e) Nível de regulação aplicável ao mercado dos serviços e/ou produtos objeto da contratação; e
f) Se o Terceiro, em decorrência dos serviços a serem contratados, terá poderes de agir em nome da Onze.

11.6.4. Due diligence baseada em risco

A partir da classificação de risco atribuída, os procedimentos de diligência adicionais para avaliação do Terceiro serão definidos pelos membros da Área de *Compliance*, em caso de Terceiro de baixo risco, e pelo Diretor de *Compliance*, em caso de Terceiros de alto ou médio risco.

Caso sejam identificadas *red flags* em relação ao Terceiro, em qualquer momento do processo de *due diligence*, a Área de *Compliance* deverá avaliar a importância dessas *red flags* para solicitar ao Terceiro qualquer informação ou providência adicional que seja considerada pertinente.

11.6.4.1. Baixo Risco

Caso o Terceiro seja considerado de baixo risco e não sejam identificadas *red flags* em relação a ele, a Área de *Compliance* solicitará, como único requisito adicional para a aprovação, que o Terceiro comprove o cumprimento da legislação anticorrupção, o que poderá ser feito mediante inclusão, no contrato a ser firmado entre as partes, do compromisso de cumprimento da referida legislação anticorrupção por parte do Terceiro.

11.6.4.2. Médio risco

Para os Terceiros que apresentem risco médio, o Diretor de *Compliance* poderá determinar as seguintes etapas adicionais, sem limitação, para aprovação da contratação:

(i) Solicitar a comprovação do cumprimento da legislação anticorrupção, nos termos do item 11.6.4.1 acima;

(ii) Solicitar o preenchimento de um questionário de *due diligence*; iii) Solicitar uma ou mais das seguintes providências (com base não apenas no nível de risco atribuído, mas também a partir das respostas do Terceiro ao questionário de *due diligence*):

a. Comprovar as referências comerciais fornecidas pelo Terceiro;
b. Solicitar um relatório comercial sobre o Terceiro;
c. Realizar buscas, em bancos de dados públicos, de registros corporativos, relatórios de crédito, pedidos de recuperação judicial ou falência e litígios envolvendo o Terceiro;
d. Realizar uma visita na sede o Terceiro ou, não sendo viável a visita, obter evidências da legitimidade das operações do Terceiro;
e. Solicitar a uma empresa especializada a preparação de relatório básico de *due diligence* sobre o Terceiro; e/ou
f. Realizar uma entrevista com o Terceiro ou seu representante.

11.6.4.3. Alto risco

Para os Terceiros cujo risco seja considerado alto, o Diretor de *Compliance* poderá solicitar, além das etapas adicionais previstas no item 6.4.2 acima, a elaboração, por empresa especializada, de relatório avançado de *due diligence* sobre o Terceiro.

11.6.5. Aprovação ou reprovação da contratação

Após a realização do processo de *due diligence*, o Diretor de *Compliance* deverá aprovar ou reprovar o Terceiro. Esta aprovação é pré-requisito para que possa ser estabelecida uma relação comercial com o Terceiro.

Para deliberar sobre a aprovação ou não do Terceiro, o Diretor de *Compliance* avaliará:

a) Toda a informação e documentação sobre o Terceiro obtidas durante o processo de *due diligence*;
b) Os riscos envolvidos na relação proposta com o Terceiro; e
c) As *red flags* identificadas durante o processo de *due diligence*, incluindo a medidas tomadas pelo Terceiro para sanar ou atenuar as respectivas *red flags.*

Caberá sempre ao Diretor de *Compliance* tomar a decisão final sobre a aprovação ou reprovação do Terceiro.

11.6.6. Requisitos mínimos do contrato

A Área de *Compliance* deverá garantir que todas as contratações de Terceiros sejam firmadas por meio de contratos escritos que:

a) Descrevam de forma específica os serviços que serão prestados e todas as condições de pagamento;
b) Incluam disposições adequadas em relação ao cumprimento das normas anticorrupção, incluindo a proibição de pagamentos indevidos, direito de auditoria, direito de término do contrato e obrigações de treinamento; e
c) Incluam salvaguardas apropriadas de segurança da informação.

A Área de *Compliance* deverá garantir que o Terceiro não inicie a prestação dos serviços contratados antes da (1) avaliação por meio do processo de *due diligence*; (2) aprovação do Diretor de *Compliance*; e (3) celebração do contrato.

11.7. Red Flags

No processo de seleção e contratação de Terceiros, a Onze deverá verificar a ocorrência de circunstâncias que sinalizam risco de práticas de corrupção por parte do Terceiro. Tais circunstâncias são denominadas *red flags*. A presença de *red flags* sugere a necessidade de maior escrutínio e salvaguardas contra possíveis violações causadas pelo Terceiro.

A seguir, segue lista não exaustiva das principais *red flags* a que a Onze deve estar atenta:

i) A remuneração do Terceiro é excessiva em comparação com os parâmetros de mercado;
ii) O Terceiro prevê, nos instrumentos contratuais, de forma vaga e imprecisa os serviços a serem prestados;
iii) O Terceiro atua preponderante em linha de negócios distinta daquela para a qual está sendo contratado;
iv) O Terceiro apresenta reputação ruim ou duvidosa, ou antecedentes negativos;
v) O Terceiro é um agente público atualmente ou o foi no passado, ou é controlado por um agente público;
vi) O Terceiro tem uma relação pessoal ou familiar próxima ou uma relação comercial com um agente público ou seus familiares;
vii) O Terceiro foi sugerido por um agente público, especialmente se o agente público exerce cargo em órgão ou agência governamental a que a Onze e seus negócios estejam sujeitos;
viii) O Terceiro se opõe às declarações de cumprimento da legislação anticorrupção nos contratos;

ix) O Terceiro solicita termos contratuais não usuais ou formas de pagamento que podem acarretar problemas em relação ao cumprimento da legislação local, como o pagamento em dinheiro, em moeda estrangeira, em conta bancária *offshore*;

x) O Terceiro solicita o pagamento urgente ou antes do prazo previsto, de forma inesperada;

xi) O Terceiro efetua pagamentos de valores além daqueles especificados em contrato, sem motivo razoável;

xii) A *due diligence* revela que o Terceiro é uma "sociedade fantasma" ou possui alguma outra estrutura corporativa pouco transparente e incomum;

xiii) O Terceiro apresenta como qualificação unicamente a sua influência sobre agentes públicos;

xiv) O Terceiro requer sigilo em relação à sua identidade ou, caso seja uma pessoa jurídica, à identidade dos sócios, diretores e/ou colaboradores; e

xv) Os registros contábeis do Terceiro são pouco transparentes.

Em regra, qualquer fato verificado pela Onze que possa por em dúvida se o Terceiro está efetivamente oferecendo a contratação de um serviço necessário a um preço de mercado é uma *red flag*. Caso o processo de *due diligence* identifique qualquer *red flag*, uma investigação mais apurada poderá ser determinada. A constatação de uma *red flag* após a contratação do Terceiro deverá ser informada ao Diretor de *Compliance* para que avalie o caso e tome as medidas que entender cabíveis.

11.8. Monitoramento

Após a contratação dos Terceiros, a Área de *Compliance* realizará o acompanhamento e a supervisão de suas atividades, devendo estar sempre atenta a eventuais sinais de alerta ou de descumprimento às políticas internas da Onze e à legislação e regulamentação aplicável.

11.8.1. Supervisão baseada em risco

A Onze realizará supervisão baseada em risco dos Terceiros contratados, com a finalidade de destinar maior atenção aos Terceiros que demonstrem maior probabilidade de apresentar falhas em sua atuação ou representem potencialmente um dano maior para os investidores e para a integridade do mercado financeiro e de capitais.

Para os Terceiros classificados como sendo de baixo risco, a Área de *Compliance* realizará a supervisão por meio das seguintes medidas:

i) Solicitar a justificativa e a documentação pertinente antes de efetuar o pagamento de qualquer despesa requerida pelo Terceiro;

ii) Verificar se todos os encargos, tarifas ou despesas de qualquer natureza estão previstos em contrato ou na legislação;
iii) Observar a existência de questões não usuais ou excessivas, conforme os parâmetros de mercado, em relação à execução do contrato;
iv) Verificar a existência de fundados indícios de que o Terceiro realizou ou realizará pagamentos potencialmente considerados ilícitos e, em caso positivo, notificar o Diretor de *Compliance* para que tome as medidas cabíveis.

Adicionalmente, a Onze realizará, a cada 36 (trinta e seis) meses, a reavaliação da classificação de risco desses Terceiros e o respectivo processo de *due diligence* pertinente.

Para os Terceiros classificados como sendo de médio ou alto risco, além das medidas descritas acima, a Área de *Compliance* também deverá:

i) Solicitar periodicamente comprovações de cumprimento das leis anticorrupção;
ii) Reunir-se periodicamente com o Terceiro para discutir o desempenho dos serviços contratos e as expectativas da Onze em relação ao desempenho, devendo o teor das discussões ser formalizado em ata; e
iii) Quando aplicável, tendo em vista os riscos específicos associados ao Terceiro, exercer o direito de auditar os livros, registros e atividades comerciais do Terceiro.

As medidas acima descritas deverão ser realizadas, no mínimo, a cada 24 (vinte e quatro) meses, para os Terceiros considerados de médio risco, e a cada 12 (doze) meses para os Terceiros considerados de alto risco. Na mesma periocidade, será realizada a reavaliação da classificação de risco desses Terceiros e o respectivo processo de *due diligence* pertinente.

11.9. Violações e Sanções Aplicáveis

É de responsabilidade de todos os Colaboradores (próprios e de Terceiros) comunicar qualquer violação e suspeita de violação aos requisitos desta Política. As comunicações de violação e suspeita de violação, identificadas ou anônimas, podem ser feitas diretamente ao Diretor de *Compliance*.

As sanções decorrentes do descumprimento dos princípios estabelecidos nesta Política serão definidas e aplicadas pelo Diretor de *Compliance*, a exclusivo critério desta, garantido ao Colaborador, contudo, amplo direito de defesa.

Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente no País à época do fato, sem prejuízo do direito da Onze de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

12. PLANO DE CONTINUIDADE DO NEGÓCIO

Na execução de suas atividades, a Onze está sujeita a riscos relacionados à ocorrência de eventos que possam comprometer, dificultar ou mesmo impedir a continuidade das operações da Onze, tais como catástrofes naturais, ataques cibernéticos, sabotagens, roubos, vandalismos e problemas estruturais.

Este plano de continuidade do negócio busca descrever os procedimentos, estratégias, ações e infraestrutura empregados pela Onze para garantir a continuidade das suas atividades em situações de contingência.

O responsável pelo cumprimento do plano de continuidade do negócio e pela ativação do plano de contingência é o Diretor de *Compliance*.

12.1. Estrutura e procedimentos de contingência

A Onze garantirá a continuidade de suas operações no caso de um desastre ou qualquer outra interrupção drástica dos negócios.

Os servidores da Onze são virtuais via *cloud*, de forma que todas as informações podem ser acessadas remotamente de qualquer lugar com acesso à internet.

Em caso de emergência na sede da Onze que impossibilite o seu uso, os Colaboradores trabalharão remotamente, em um *site* de contingência devidamente adaptado para receber os Colaboradores com funções chave.

Todos os colaboradores possuem uma cópia do plano de continuidade do negócio que descreve todas as ações a serem seguidas em caso de desastre.

12.2. Plano de contingência

O plano de contingência será acionado toda vez que, por qualquer motivo, o acesso às dependências da Onze fique inviabilizado.
Nesses casos, os Diretores de *Compliance* e de Gestão, de comum acordo, devem determinar a necessidade do trabalho remoto, no ambiente residencial do Colaborador ou

em lugar a ser definido na oportunidade, o qual possua conexão própria e segura, sendo utilizado o notebook da Onze, seguindo as regras abaixo:

(i) Nos primeiros 60 minutos de impossibilidade do acesso, um Colaborador de cada área da Onze deve estar apto e preparado para iniciar os trabalhos por meio de acesso remoto;
(ii) Após esse período, caso a impossibilidade de acesso permaneça, cada um dos Colaboradores designados deverá realizar sua função remotamente, garantindo a continuidade das atividades da Onze.

Os Diretores de Gestão e de *Compliance* serão responsáveis por determinar o Colaborador de sua respectiva área que deverá assumir a posição de trabalho por acesso remoto.

Após a normalização do acesso à Onze, os Colaboradores deverão apresentar ao Diretor de *Compliance* relatório das atividades executadas durante o período de contingência.

12.3. Atualização do plano de continuidade do negócio

Os procedimentos, estratégias e ações constantes do plano de continuidade do negócio serão testados e validados, no mínimo, a cada 12 (doze) meses, ou em prazo inferior, se exigido pela regulamentação em vigor.

13. SEGURANÇA CIBERNÉTICA

A Onze adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é o Diretor de Compliance.

13.1. Avaliação dos riscos

No exercício das suas atividades, a Onze poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

i) *Malwares*: softwares desenvolvidos para corromper computadores e redes:
   a. Vírus: software que causa danos à máquina, rede, outros softwares e bancos de dados;

b. Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
c. *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
d. *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoas e número de cartão de crédito:
a. *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
b. *Phishing*: links transmitidos por e-mails, simulando se uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

13.2. Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, a Onze adota as seguintes medidas de prevenção e proteção:

i) Controle de acesso adequado aos ativos da Onze, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos da Onze;

ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis;

iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

iv) Rotinas de backup;

v) Criação de logs e trilhas de auditoria sempre que permitido pelos sistemas;

vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;

vii) Implementação de recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais; e

viii) Restrição à instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

No que diz respeito à segurança cibernética, a Onze possui filtros de e-mail Mimecast, firewall Palo Alto PA 220 e anti-vírus Traps. Ademais, a Onze faz uso do *OneDrive* integrado ao AWS Amazon, que contempla testes periódicos de segurança, rotinas de monitorameno, contingenciamento e backup; além de fazer monitoramento do fluxo de rede continuamente ativo e baseado em heurística e a mitigação em linha contra os ataques de DDoS mais comuns e que ocorrem mais frequentemente nas camadas de rede e transporte.

13.3. Monitoramento

A Onze possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Onze mantém inventários atualizados de hardware e software, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Onze, como computadores não autorizados ou softwares não licenciados.

Além disso, a Onze mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de backup são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a Onze analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

13.4. Plano de resposta

Caso seja identificado um potencial incidente relacionado à segurança cibernética, o Diretor de *Compliance* deverá ser imediatamente comunicado. O *Diretor de Compliance* deverá comunicar o fato, de imediato, aos Sócios da Onze.

Num primeiro momento, o Diretor de *Compliance* se reunirá com os demais diretores da Onze para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Onze, serão tomadas, em conjunto com os assessores de tecnologia da informação da Onze, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Onze, serão observados os procedimentos previstos no plano de continuidade do negócio, descrito no item 11 acima.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Onze.

13.5. Reciclagem e revisão

A Onze manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

O Diretor de *Compliance*, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

ANEXO I - Termo de Adesão

Eu, ..., portador da Cédula de Identidade nº ..... e/ou Carteira de Trabalho e Previdência Social nº ..... série ....., declaro para os devidos fins que:

1. Estou ciente da existência do "Manual de Controles Internos *(compliance)*" da Onze ("Manual de Compliance") e de todas as políticas internas da Onze, inclusive o "Código de Ética", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" ("Políticas Internas"), que recebi, li e tenho em meu poder.

2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela Onze, e comprometo-me a comunicar, imediatamente, aos diretores da Onze qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.

3. Tenho ciência e comprometo-me a observar integralmente os termos da política de confidencialidade estabelecida no Manual de *Compliance* da Onze, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.

4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigome a ressarcir qualquer dano e/ou prejuízo sofridos pela Onze e/ou os respectivos sócios e diretores, oriundos do não-cumprimento do Manual de *Compliance* e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.

5. Participei do processo de integração e treinamento inicial da Onze, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Onze, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.

6. As normas estipuladas no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de

qualquer outra norma mencionada pela Onze, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.

7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei a Onze a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual de *Compliance*, salvo conflitos decorrentes de participações em outras empresas, descritos na "Política de Investimento Pessoal", os quais tenho ciência que deverão ser especificados nos termos previstos no Manual de *Compliance*:

_____

_____

_____

_____

_____

_____

_____

São Paulo, ... de ..... de 20..... .

_____

[DECLARANTE]

ANEXO II - Solicitação para Desempenho de Atividade Externa

1. Nome da instituição na qual será realizada a Atividade Externa / descrição da Atividade Externa:

2. Você terá uma posição de diretor ou administrador? [ ] sim [ ] não

3. Descreva suas responsabilidades decorrentes da Atividade Externa:

4. Tempo estimado que será requerido de você para desempenho da Atividade Externa (em bases de horas mensais):

5. Você ou qualquer parte relacionada irá receber qualquer remuneração ou contraprestação pela Atividade Externa: [ ] sim [ ] não

Se sim, descreva:_____.

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da Onze, e que não interfere com suas atividades na Onze, não compete ou conflita com quaisquer interesses da Onze. O Colaborador declara e garante, ainda, que irá comunicar ao Diretor de *Compliance* da Onze quaisquer conflitos de interesses que possam surgir com relação à Atividade Externa acima descrita.

São Paulo, _____ de _____ de 20_____.

_____

[Colaborador]

Resposta do Diretor de *Compliance:* [ ] Solicitação Aceita [ ] Solicitação Negada

_____

Diretor de *Compliance*

ANEXO III – Classificação de Pessoa Exposta Politicamente

De acordo com a Resolução CVM 50, considera-se como Pessoa Exposta Politicamente, as pessoas definidas abaixo:

I. Os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
II. Os ocupantes de cargo, no Poder Executivo da União, de:

a) Ministro de Estado ou equiparado;
b) Natureza Especial ou equivalente;
c) presidente, vice-presidente e diretor, ou equivalentes, de entidades da administração pública indireta; e
d) Grupo Direção e Assessoramento Superiores (DAS), nível 6, ou equivalente;

III. Os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;
IV. Os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal;
V. Os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;
VI. Os presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;
VII. Os Governadores e os Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Tribunais Militares, Tribunais de Contas ou equivalentes dos Estados e do Distrito Federal; e
VIII. Os Prefeitos, os Vereadores, os Secretários Municipais, os presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas ou equivalentes dos Municípios.
IX. São também consideradas expostas politicamente as pessoas que, no exterior, sejam:

a) I – chefes de estado ou de governo;
b) II – políticos de escalões superiores;

c) III – ocupantes de cargos governamentais de escalões superiores;
d) IV – oficiais-generais e membros de escalões superiores do Poder Judiciário;
e) V – executivos de escalões superiores de empresas públicas; ou
f) VI – dirigentes de partidos políticos.

X. Dirigentes de escalões superiores de entidades de direito internacional público ou privado.

A condição de pessoa exposta politicamente perdura até 5 (cinco) anos contados da data em que a pessoa deixou de se enquadrar nos critérios acima.

Para fins do disposto nesse Anexo, são considerados:

a) Familiares: os parentes, na linha direta, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada; e
b) Estreitos colaboradores:

- pessoas naturais que são conhecidas por terem sociedade ou propriedade conjunta em pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, que figurem como mandatárias, ainda que por instrumento particular, ou possuam qualquer outro tipo de estreita relação de conhecimento público com uma pessoa exposta politicamente; e
- pessoas naturais que têm o controle de pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de uma pessoa exposta politicamente.