Monetus

Manual de Controles Internos e Compliance

Introdução

Monetus Investimentos

A Monetus Investimentos LTDA. é uma gestora de investimentos, constituída em 05/03/2012. A empresa foi criada com o intuito de prestar o serviço de administração de carteiras de títulos e valores mobiliários de terceiros e gestão de fundos de investimento.

Atividades da empresa

A Monetus Investimentos atua com a gestão de carteiras de valores mobiliários e a gestão de fundos de investimentos. A Monetus Investimentos opera os seguintes produtos financeiros:

- Ações
- Títulos públicos
- Debêntures
- Cotas de fundos de investimentos
- Fundos de investimentos imobiliários
- Bônus de subscrição
- Títulos emitidos por instituições financeiras (CDBs, LCs, LFs, DPGEs, entreoutras).

Manual

Este Manual de Regras, Procedimentos e Controles Internos, teve sua elaboração com o objetivo de cumprir os requisitos da Instrução 558 da Comissão de Valores Mobiliários. Com isso, o documento visa a assegurar o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional. Assim, o Manual contém as seguintes políticas ou informações:

- Políticas de Confidencialidade;
- Política de Segurança Cibernética e Proteção de Informações Sigilosas;
- Políticas de Treinamento; e
- Políticas de Segregação das Atividades.

Adesão ao Manual

O Manual, bem como as outras normas e políticas dA Monetus Investimentos, é exposto a todos os funcionários da entidade por ocasião de ingresso, que devem assinar o Termo de Adesão ao Manual de Regras, Procedimentos e Controles Internos (Anexo 1 – Termo de Adesão ao Manual) comprovando ter ciência das normase regras internas da entidade. Ainda, o conteúdo do Manual deve ser reiterado com os funcionários com frequência mínima anual.

- Atualização do Manual

Este Manual de Regras, Procedimentos e Descrição dos Controles Internos deve ser revisto frequentemente, pelo menos a cada dois anos, pelos sócios administradores da Monetus Investimentos, ou qualquer ocasião em que sejam identificadas alterações na regulamentação ou legislação aplicável à atividade econômica dA Monetus Investimentos.

Setor de *Compliance*

- Definição

Compliance significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para um determinado negócio ou operação. É a atividade de assegurar que a empresa está cumprindo à risca todas as imposições dos órgãos de regulamentação, dentro de todos os padrões exigidos de seu segmento. E isso vale para as esferas trabalhista, fiscal, contábil, financeira, ambiental, jurídica, previdenciária, ética, etc.

- Objetivo

A Monetus Investimentos adota o seguinte setor com o objetivo de estabelecer e fiscalizar rotinas internas que assegurem o verdadeiro cumprimento pelos funcionários da entidade das normas de conduta às quais se encontra sujeita, visando, assim, a orientar as atividades de *Compliance* de modo a atestar que os funcionários dA Monetus Investimentos estejam agindo dentro dos padrões éticos.

- Atuação

Diretor de *Compliance* e os funcionários que atuem na área devem executar as suas atribuições e/ou obrigações com soberania, possuindo total acesso às informações e documentos relativos às atividades da entidade, de forma que seja possível aferir o cumprimento das leis e regras estabelecidas internamente.

Além disso, os profissionais devem manter uma postura ativa, com o propósito de zelar pelo cumprimento das leis e regras em vigor sobre todos os funcionários dA Monetus Investimentos.

- Declaração de ciência

Ao final deste Manual de *Compliance*, o Diretor de *Compliance* deve assinar o Termo de Ciência (Anexo 2 – Termo de Ciência das Regras Internas), certificando o conhecimento das amplas regras internas que objetivam manter a íntegra relação de confiança entre a entidade e os outros membros do mercado aqui expostas.

Política de Confidencialidade

- Confidencialidade

A Monetus Investimentos tem de tratar com informações sigilosas de atuais e potenciais clientes de acordo com a natureza de suas atividades.

Desta forma, e para preservar a privacidade de informações pessoais ou financeiras de clientes e parceiros, é estabelecido que fica vedada a divulgação de qualquer informação de caráter confidencial de transações, como dados, comunicados e quaisquer outras informações relacionadas a clientes, *know-how*, e técnicas utilizadas pela Monetus Investimentos.

Esta vedação é aplicável a todos os colaboradores da empresa, que devem sempre zelar pela confidencialidade de todas as informações que tiverem acesso e que tenham sido obtidas em função das atividades que eles desempenham dentro da Monetus Investimentos, por prazo indeterminado.

Da mesma forma, toda e qualquer informação obtida que seja decorrente da atividade empresarial realizada dentro dA Monetus Investimentos não deve ser divulgada, sob nenhuma hipótese, a terceiros não colaboradores.

Isso se aplica também às estratégias de investimentos, relatórios e estudos promovidos pela área de análise e gestão de investimentos, opiniões sobre ativos financeiros extraídas internamente, etc.

Para complementar os termos expostos acima, é estabelecido que todos os papeis e documentação relacionados à empresa e seus clientes deverão ser mantidos em local seguro, para que o risco de que pessoas não autorizadas venham a ter acesso a informações confidenciais seja minimizado.

Por fim, é estabelecido que os colaboradores da empresa não estão autorizados a discutir informações confidenciais em locais públicos ou através de telefones celular, aplicativos de mensagens de texto ou viva-voz.

- Termo de Confidencialidade

É obrigatória a assinatura de um "Termo de Confidencialidade" (Anexo 3 – Termo de Confidencialidade) por todos os funcionários que venham a ingressar na Monetus Investimentos, que engloba políticas de uso, concessão e fiscalização de recursos de telefonia, informática e internet. Caso não ocorra o cumprimento do "Termo de Confidencialidade", os funcionários estão sujeitos a sanções analisadas pelas Diretoria de *Compliance*, além de responder nos âmbitos cível e criminal.

- Permissão de Manifestações

Em caso de imposições de autoridades governamentais ou em casos de decisões judiciais, arbitrais ou administrativas, o respectivo funcionário deverá, primeiramente, reportar o Diretor de *Compliance* para que assim este defina sobre o modo mais apropriado para tal revelação.

- Proibições

É expressamente proibido que os funcionários da Monetus Investimentos sem qualquer prévia permissão por escrito da Monetus Investimentos:

- transmitir dados, físicos ou eletrônicos, além da transferência de informações sigilosas para terceiros relativas aos clientes e atividades em que a Monetus Investimentos opera;
- autorizar o acesso de terceiros a infraestrutura de informações ou operações e sistema de bancos de dados de incumbência e/ou posse da Monetus Investimentos;
- realizar cópias de documentos registrados em arquivos, papel ou meio magnético, que incluam dados da Monetus Investimentos, ou informações pertencentes a clientes e parceiros da entidade;
- extrair do local de trabalho qualquer tipo de material da Monetus Investimentos, incluindo dados financeiros sobre transações de clientes da entidade.

Política de Segurança Cibernética e Proteção de Informações Sigilosas

- Introdução

A Política de Segurança Cibernética e Proteção de Informações Sigilosas da Monetus Investimentos é uma declaração formal da gestora para com o compromisso com a segurança cibernética (*cybersecurity*) e a proteção de informações sigilosas, conforme definição adiante, devendo ser cumprida por todos os colaboradores da empresa.

- Objetivo

A Política de Segurança Cibernética e Proteção de Informações Sigilosas é implementada e controlada por um Comitê de Gestão de Riscos, compostos pelos seguintes membros: Diretoria de Risco, Diretoria de *Compliance, Diretoria de Tecnologia* e funcionários de ambas as áreas indicados pelas respectivas Diretorias.

Essa política tem como objetivo principal aprimorar a segurança cibernética e garantir a proteção das informações sigilosas mantidas pelo Monetus, nos termos do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, seguindo as recomendações da ANBIMA, e da Instrução CVM nº 558.

Em suma, nenhuma informação sigilosa deve ser divulgada, seja dentro ou fora das instalações físicas da empresa, a qualquer pessoa que não necessite ou não deva ter acesso à essas informações para desempenhar as suas atividades profissionais.

Na ausência de previsão expressa, o fornecimento de informações sigilosas poderá ocorrer somente com o conhecimento e autorização prévia do Diretor de Gestão de Riscos e Compliance.

- Aplicação e Responsabilidades

A efetividade da Política de Segurança Cibernética e Proteção de Informações Sigilosas da Monetus depende da conscientização de todos os funcionários da empresa, bem como do esforço constante de segurança cibernética e proteção de informações sigilosas promovido por eles. Esta política deve ser conhecida e seguida por todos os colaboradores que utilizam os recursos de tecnologia disponibilizados pela Monetus, sendo de responsabilidade individual e coletiva o seu cumprimento.

Conforme dito, cabe a todos os colaboradores da empresa cumprir fielmente esta política. Caso algum colaborador tenha alguma dúvida quanto a ela, é necessário que o mesmo busque orientação de seu superior imediato sobre como prosseguir com a boa aplicação da política. Cabe aos colaboradores cumprir as leis e normas de direito autoral e propriedade intelectual no que se refere às informações sigilosas, proteger as informações sigilosas contra acesso, modificação, destruição, divulgação e distribuição não autorizadas, e assegurar que os recursos de tecnologia serão usados apenas para as finalidades permitidas pela Monetus.

A área de Compliance é responsável pelo monitoramento contínuo dos resultados dos testes de segurança realizados e pelo registro de potenciais desvios desta política. Além disso, o Diretor de Compliance é responsável por estabelecer quais são as permissões e restrições de acesso

de qualquer colaborador da empresa de acordo com a sua posição funcional.

Por fim, cabe aos colaboradores da empresa comunicar imediatamente o Diretor de Compliance caso seja identificado qualquer descumprimento ou violação de qualquerponto desta política.

- Conceitos e Princípios

Todas as informações sigilosas são ativos de valor para a Monetus. Consequentemente, elas precisam ser devidamente protegidas contra ameaças e ações potencialmente danosas para nossos clientes do serviço de carteira administrada, fundos, colaboradores e a própria empresa.

Essas informações podem ser armazenadas e transmitidas de diferentes maneiras, como, por exemplo, arquivos eletrônicos, mensagens instantâneas, websites,
bancos de dados, impressões físicas, mídias e outros. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, remoção, alteração e eliminação de seu conteúdo.

A adoção da Política de Segurança Cibernética, bem como procedimentos que garantam que a política está sendo cumprida, é uma prioridade constante da Monetus, reduzindo assim os riscos de falhas, bem como danos e prejuízos que possam comprometer os objetivos e a imagem da empresa.

Assim, por princípio, a guarda e segurança das Informações Sigilosas deve abranger três aspectos básicos, destacados a seguir:

- Restrição de Acesso: Somente pessoas devidamente autorizadas pela Gestora devem ter acesso às Informações Sigilosas;
- Integridade das Informações: Somente alterações, supressões e adições autorizadas pela Gestora devem ser realizadas às Informações Sigilosas;
- Disponibilidade das Informações: As Informações Sigilosas devem estar facilmente disponíveis para os Colaboradores autorizados sempre que necessário ou fordemandado.

Para assegurar os aspectos acima, as Informações Sigilosas são adequadamente protegidas e gerenciadas contra furto, fraude, espionagem, perda, acidentes e outras ameaças potencialmente danosas.

Em cumprimento ao Guia Anbima de Segurança Cibernética de dezembro de 2017 (2ª edição), a Monetus possui cinco pilares principais no seu programa de segurança cibernética:

- Identificação e avaliação de riscos (risk assessment);
- Ações de prevenção e proteção;
- Monitoramento e testes;
- Plano de resposta; e
- Reciclagem e revisão.

A implantação e monitoramento da capacidade da Gestora atender a estes pilares deverá ser feito pelo Diretor de Gestão de Riscos e de Compliance. Também a fim de atingir os objetivos dispostos acima, cada segmento de atuação da Gestora terá suas próprias responsabilidades.

É de obrigação do Diretor de Gestão de Riscos e de Compliance promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de informações sigilosas, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

- Procedimentos de Segurança Cibernética

A seguir estão descritos os procedimentos relacionados ao bom cumprimento dos cincopilares sugeridos pelo Guia de Cibersegurança da ANBIMA.

- Identificação e Avaliação de Riscos (*Risk Assessment*)

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os tipos de ataques cibernéticos mais comuns utilizados por criminosos são os seguintes:

a. *Malwares* - softwares desenvolvidos para corromper computadores e redes, como vírus, *trojanhorses, spywares* e *ransomwares;*
b. Engenharia Social – métodos de manipulação social e psicológica para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;
   - *Pharming* – direcionamento do usuário para um site fraudulento (falso), sem o conhecimento do usuário;
   - *Phishing scam* – links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obterinformações confidenciais;
   - *Vishing* – simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
   - *Smishing* – simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; 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.
c. 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.
d. Invasões (*advanced persistente threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

A avaliação de risco envolve a identificação de todos os processos, pontos de contato e informações possivelmente afetadas por ataques dos mais diversos tipos. A Monetus Investimentos utiliza uma versão adaptada do modelo de segurança cibernética do CIS Controls, seguindo metodologia própria focada nas necessidades da gestora, bem como partes de modelos diferentes, também provenientes de modelos amplamente reconhecidos e eficazes, conforme instruções presentes do

documento “Noções Básicas sobre o Programa de Segurança Cibernética” da ANBIMA.

- Ações de Prevenção e Proteção

A Gestora adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao desempenho profissional do usuário.

O acesso físico às áreas com informações críticas, sensíveis e/ou sigilosas, como documentos, contratos e afins, também é restrito, e é concedido apenas quando necessário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados. As senhas de acesso também são modificadas periodicamente, conforme política interna. Todos os colaboradores utilizam um gerenciador e cofre de senhas de acesso seguro ativamente criptografado, garantindo assim a segurança de acesso às diferentes plataformas necessárias.

Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A Monetus também conta com recursos anti-malware nas estações e servidores de rede, como antivirus e firewalls pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

A Monetus realiza, também, backup periódico das informações e dos diversos ativos da instituição, conforme política interna, respeitando as boas práticas de armazenamento e proteção de informações sigilosas.

- Monitoramento e Testes:

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Gestora ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente de trabalho, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado via software e/ou hardware pela Área de Gestão de Riscos e de Compliance.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Gestora, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Gestora possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a Monetus realiza testes de segurança no seu sistema de segurança da informação e proteção de dados. Dentre as medidas, incluem-se, mas sem se limitar:

a. Verificação dos logs dos Colaboradores;
b. Alteração periódica de senha de acesso dos Colaboradores;
c. Segregação de acessos;
d. Manutenção semestral de todo os hardwares; e
e. Backup diário, realizado na nuvem.

Esses testes de segurança são realizados, no mínimo, anualmente, permitindo que a Monetus esteja sempre preparado para a continuação de suas atividades, bem como mitigando quaisquer eventuais riscos operacionais ou de imagem.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da Gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de backup são periodicamente monitoradas.

- Plano de Resposta:

Havendo indícios ou de suspeita fundamentada, o Diretor de Risco e Compliancerealizará os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo doevento.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança,inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazopossível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater o evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Monetus. Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos e de Compliance. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que sumariamente, constar no Relatório de Controles Internos.

- Reciclagem e Revisão:

A Monetus apresenta anualmente, em uma reunião com toda a equipe, asdiretrizes dessa política, com o objetivo de melhor guiar e educar os colaboradores com as boas práticas de segurança cibernética e proteção de informações sigilosas descritasnessa presente política.

Além disso, esta política também é revisada semestralmente, e alterações nas diretrizes poderão ocorrer caso seja constatada a necessidade de atualização do

conteúdo. Caso seja necessário, poderá também ser atualizada de forma tempestiva, afim de sanar quaisquer deficiências encontradas.

- Diretrizes de Segurança da Informação e Proteção de Informações Sigilosas

    a Mecanismos de Segurança e Diretrizes Gerais

    Como medida de segurança, são realizados testes de forma recorrente a fim de garantir a segurança e integridade das informações por nós mantidas. Todas as informações de caráter confidencial são restritas aos funcionários responsáveis. Se caracterizam como informação confidencial todo e qualquer documento contendo informações que possibilitem a identificação dos nossos clientes ou que não podem ser acessados por algum colaborador ou área de empresa. Todos os documentos impressos e que não necessitam arquivamento, são mantidos apenas enquanto são necessários para a execução de alguma tarefa, sendo eliminados assim que se tornam desnecessários. Além disso, em nenhuma hipótese documentos físicos com informações confidenciais podem ser mantidos em locais que colaboradores com qualquer tipo de restrição possam ter acesso.

    Todos os computadores e estações de trabalho são mantidos com senha, com o objetivo de restringir o acesso a qualquer pessoa que não seja o colaborador ou pessoa autorizada. Todas as senhas de todos os computadores e estações de trabalho são substituídas recorrentemente com o objetivo de garantir a segurança das informações contidas nos mesmos. Além disso, é mandatório a utilização do mecanismo de autenticação de dois fatores (senha + token) para acesso ao servidor da empresa, além de requerer a atualização da senha a cada 365 dias.

A Monetus Investimentos também se reserva no direito de gravar quaisquer ligações telefônicas feitas a partir dos aparelhos telefônicos fixos e móveis disponibilizados pela empresa, além das ligações feitas por meio digital (VoIP). Além disso, a área de Compliance reserva o direito de monitorar todos os conteúdos acessados no computador de cada

colaborador e verificar qualquer conversa realizada através dos servidores de e-mail da empresa.

O acesso às informações confidenciais mantidas pela empresa em meio digital ou físico por terceiros (não-funcionários) é terminantemente proibida. Caso algum profissional mude de uma área que lida com informações confidenciais para uma área que não lida com informações confidenciais, o profissional em questão perderá imediatamente o acesso à essas informações. Além disso, é terminantemente proibido o compartilhamento e a utilização de qualquer informação confidencial que o colaborador teve acesso na função anterior. Caso qualquer funcionário infrinja alguma norma relacionada à segurança das informações, o mesmo estará sujeito a ação disciplinar, podendo ocasionar até a suspensão do contrato de trabalho, após avaliação do caso pelo Diretor de Compliance.

b Cópias e Impressões Físicas de Documentos

Salvo as cópias e impressões feitas em prol da execução das tarefas, toda reprodução não autorizada é expressamente proibida, dada a natureza confidencial das informações contidas nos documentos. Sendo assim, é também expressamente proibido a utilização de quaisquer meios de armazenamento externo (CDs, DVDs, disquetes, flashdrives, HDs externos, SSDs externos, NASs, etc), bem como a conexão de equipamentos de terceiros na rede interna da empresa que não sejam usados exclusivamentepara fins de trabalho.

c Procedimentos Internos para Tratar de Casos de Vazamento de Informações Confidenciais

Em caso de vazamento de informações, o funcionário responsável será desligado da empresa, tendo o seu contrato rescindido por justa causa, conforme estabelecido no nosso Código de Ética e que todo colaborador deve atestar assim que ingressar na Monetus Investimentos.

d Regras e Boas Práticas de Comportamento Seguro:

Informações sigilosas podem ser encontradas na sede da Gestora, em meio físico e digital, e fazem parte do ambiente de trabalho de todos os colaboradores. Portanto, é fundamental para a proteção delas que os colaboradores da Monetus adotem comportamento seguro e consistente, com destaque especial para os seguintes itens:

- Os colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;
- Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das informações sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, entre outros, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
- Todo tipo de acesso aos dados e informações da Gestora, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;
- Assuntos relacionados ao desempenho de atividades e funções na Gestora não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);
- As senhas de acesso do Colaborador aos sistemas da Gestora são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros

Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;

- Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
- Somente softwares previamente aprovados pelo Diretor de Compliance podem ser instalados e usados nas estações de trabalho;
- Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ouexecutados nos computadores da Gestora;
- Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter Informações Sigilosas. Portanto, não podem ser parcial ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;
- O acesso remoto à rede, às Informações Sigilosas e sistemas da Gestora somente será permitida mediante autorização do Diretor de Gestão de Riscos e de Compliance, e desde que seja estritamente necessário para o desempenho das funções do colaborador. O colaborador será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas da Gestora;
- O Colaborador deve evitar realizar acesso remoto à rede da Gestora a partir de um dispositivo público, e, caso o faça, deverá limpar o cache e deletar todos os arquivos temporários;
- Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Gestora sem a autorização prévia do superior hierárquico do Colaborador.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar

constrangimento à terceiros, bem como com conteúdo político ou outro quepossa colocar a Gestora em risco.
Conforme descrito, o Monetus se reserva o direito de monitorar o usodos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos
documentos internos da Gestora e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

e Regras de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos:

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela Gestora são monitorados, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da Gestora, através de monitoramento a ser efetuado pela Área de Gestão de Riscos e de Compliance.
Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da Gestora deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Gestão de Riscos e de Compliance.O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a Pedido formal de concessão e cancelamento de autorização de acesso dousuário aos sistemas;
a Utilização de identificador do colaborador (em meio digital - ID do colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
a Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;
a Remoção imediata de autorizações dadas aos Colaboradores afastados oudesligados da Gestora, ou que tenham mudado de função, se for o caso; e

a Revisão periódica das autorizações concedidas.

- Endereço Eletrônico

Em cumprimento ao art. 14, II, da Instrução CVM nº 558/15, a presente Políticaestá disponível no endereço eletrônico da Gestora: https://www.monetus.com.br.

- Vigência

Esta Política revoga todas as versões anteriores e passa a vigorar na data de suaaprovação pelo Comitê de Gestão de Riscos e de Compliance. Eventual incompatibilidade entre as versões anteriores e a atual versão desta Política, se existirem, serão tratadas caso a caso pela Área de Gestão de Riscos e de Compliance.

Política de Treinamento

- Programa

- todos os funcionários devem ser submetidos à treinamentos anuais com a finalidade de capacitá-los e orientá-los em relação as normas de conduta internas e da legislação atual que impera sobre a atividade desenvolvida pela Monetus Investimentos;
- realização de treinamento pontuais caso ocorram mudanças em normas regulatórias sobre as operações efetuadas pela entidade;
- estímulo a educação continuada dos funcionários, incentivando à presença em seminários, palestras, congressos e demais atividades que agreguem valor à formação profissional do funcionário.

- Participação

Todos os funcionários devem estar presentes nos treinamentos que serão ministrados em relação as normas de condutas internas, informações regulatórias e legislação atual. Em caso de impossibilidade, o funcionário deve informar o Diretor de *Compliance* com o objetivo de fixar outra data para a realização do respectivo treinamento.

Além disso, em caso de financiamento de um programa de capacitação externo pela Monetus Investimentos, se houver qualquer tipo de ausência que não se justifique e a eventual não conclusão, o funcionário terá de ressarcir a entidade.

Política de Segregação das Atividades

- Objetivo

As atividades realizadas pela Monetus Investimentos são altamente reguladas e consistem basicamente na administração de carteiras de valores mobiliários e da gestão de fundos de investimentos.

Essas atividades exigem credenciamento específico e estão condicionadas ao cumprimento de uma série de exigências prévias e recorrentes, dentre elas a segregação total das atividades listadas acima entre si e em relação a quaisquer outras atividades que venham a ser desenvolvidas pela Monetus, como atividades do setor comercial, de prospecção de clientes, setor administrativo e contábil, e das atividades do nosso braço de educação financeira, a Monetus.

A Política de Segregação das Atividades da empresa visa nortear a segregação das atividades entre o time de Gestão e os outros times da empresa, definindo estrutura e procedimentos gerais que deverão ser observados por todos os colaboradores do Monetus, e, assim, eliminando quaisquer possíveis conflitos de interesse que possa haver entre os diferentes times da empresa.

- Estrutura

Todas as informações pertinentes ao time de Gestão são confidenciais e devidamente preservadas ao acesso restrito dos profissionais da área, conforme descrito na Política de Segurança Cibernética e Proteção de Informações Sigilosas.

Documentos, planilhas e softwares utilizados por profissionais deste setor são protegidos com senha e possuem o acesso monitorado pela área de Compliance, através de trilhas de auditoria.

Ademais, todos os profissionais desta área são alocados para desempenhar suas funções em local fisicamente segregado dos demais colaboradores.

Por fim, os profissionais da área de análise e gestão ainda possuem diretórios de rede privativos e restritos, bem como equipamentos computacionais devidamentesegregados das demais áreas da empresa.

Esse formato utilizado atualmente pela Monetus para a eficaz segregação das atividades permite que, caso a empresa venha a exercer quaisquer outras atividades no mercados financeiro e de capitais, tais atividades, se assim exigido pela regulamentação aplicável, sejam facilmente segregadas das atividades atuais, de formaque a segurança das suas atividades de administração de carteiras de valores mobiliários e gestão de fundos de investimentos seja sempre mantida.

- Conduta

Para regras e procedimentos a serem seguidos quanto à devida conduta esperada dos colaboradores da Monetus, temos a Política de Segurança Cibernética e Proteção de Informações Sigilosas, que diz respeito à proteção das informações sigilosas e às medidas de segurança cibernética adotadas pela empresa, e o Manual de Regras, Procedimentos e Descrição dos Controles Internos, que descreve detalhadamente os pontos principais esperados da conduta dos colaboradores daempresa.

Somado a isso, o colaborador que, a qualquer tempo, no desempenho de suas funções na Monetus, vislumbrar a possibilidade de ocorrência de uma situação deconflito de interesses com as atividades da Monetus deverá comunicar imediatamente à equipe de Compliance, nos termos do Código de Ética da empresa.

O conhecimento de qualquer infração ou indício de infração das regras contidas nesta Política deve ser imediatamente comunicado ao Diretor de Compliance para adoção das devidas providências. A violação desta política sujeitará o infrator às medidas previstas no Código de Ética da Monetus.

Em caso de dúvidas quanto aos princípios e responsabilidades descritas nesta Política, o Colaborador deve entrar em contato com o Diretor de Compliance.

A aplicação das regras aqui descritas é de responsabilidade da equipe de Compliance.

ANEXO 1 – TERMO DE ADESÃO AO MANUAL

Termo de Adesão ao Manual

Declaro que tenho ciência do conteúdo do Manual de Regras, Procedimentos e Descrição dos Controles Internos dA Monetus Investimentos, com o qual estou de acordo e ao qual atesto minha adesão, comprometo-me a cumpri-lo de forma ativa na minha posição de funcionário dA Monetus Investimentos. Declaro também que tenho ciência de que o Manual poderá sofrer alterações e atualizações periódicas, sendo certo que se manterão os efeitos da presente adesão às suas novas versões caso eu não informe por escrito a respeito de minha não concordância e adesãoàs novas versões do Manual.

_____ _____

Assinatura do Funcionário Assinatura do Diretor de *Compliance*

Data:

Nome do colaborador: RG:

CPF:

ANEXO 2 – TERMO DE CIÊNCIA DAS REGRAS INTERNAS

Termo de Ciência das Regras Internas

Na responsabilidade de Diretor de *Compliance* dA Monetus Investimentos, declaro pleno conhecimento da totalidade das regras internas que objetivam manter a relação de confiança entre a entidade e outros membros do mercado contidas no Manual de Regras, Procedimentos e Descrição dos Controles Internos e demais documentos que orientam a atuação dA Monetus Investimentos.

Assinatura do Diretor de *Compliance*

Assinatura de Testemunha

Data:

Nome do Diretor:RG:

CPF:

ANEXO 3 – TERMO DE CONFIDENCIALIDADE

Termo de Confidencialidade

Declaro que tenho ciência do conteúdo do Termo de Confidencialidade dA Monetus Investimentos, com o qual estou de acordo e ao qual atesto minha adesão, comprometo-me a cumprir todas as políticas de uso, concessão e fiscalização da entidade de forma ativa na minha posição de funcionário dA Monetus Investimentos. Declaro também que tenho ciência de que o Manual poderá sofrer mudançase atualizações frequentes, sendo certo que se manterão os efeitos da presente adesão às suas novas versões caso eu não informe por escrito a respeito de minha não concordância e adesão às novas versões do Manual.

_____ _____

Assinatura do Funcionário Assinatura do Diretor de *Compliance*

Data:

Nome do colaborador: RG:

CPF: