ADAMCAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

Data de Aprovação: 27.12.2017

Versão: 1.2

ÍNDICE

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

1. Apresentação

A Política de Segurança das Informações ("Política") da ADAMCAPITAL GESTÃO DE RECURSOS LTDA. ("Sociedade") é uma declaração formal da Sociedade acerca do seu compromisso com a proteção de Informações Sigilosas, devendo ser cumprida por todos os Colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Sigilosas.

2. Conceitos e Princípios

Todas as Informações Sigilosas constituem ativos de valor para a Sociedade, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Sociedade, Clientes, Fundos, Carteiras e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve ser prioridade constante da Sociedade, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Sociedade.

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

(i) Acesso: Somente pessoas devidamente autorizadas pela Sociedade devem ter acesso às Informações Sigilosas;
(ii) Integridade: Somente alterações, supressões e adições autorizadas pela Sociedade devem ser realizadas às Informações Sigilosas; e
(iii) Disponibilidade: As Informações Sigilosas devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

3. Objetivos

Esta Política visa proteger as Informações Sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme art. 4º, §8º, da Instrução CVM n.º 558/15.

Sendo assim, nenhuma Informação Sigilosa deve ser divulgada, dentro ou fora da Sociedade, a quem não necessite de, ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação, independentemente de ser considerada Informação Sigilosa, seja sobre a Sociedade, relativa às suas atividades, aos seus sócios, Fundos, Carteiras e Clientes dentre outras, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza conforme previstos nos documentos internos da Sociedade. Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização do Diretor de Gestão de Riscos e de *Compliance*.

4. Aplicação

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Sigilosas e dos Ativos disponibilizados pela Sociedade ao Colaborador.

A Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Sociedade, sendo de responsabilidade individual e coletiva o seu cumprimento.

5. Responsabilidades na Gestão da Política

Cabe a todos os Colaboradores:

a) Cumprir fielmente esta Política;

b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Sigilosas;

c) Proteger Informações Sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Sociedade;

d) Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela Sociedade;

e) Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Sigilosas; e

f) Comunicar imediatamente a Área de Gestão de Riscos e de *Compliance* sobre qualquer descumprimento ou violação desta Política.

6. Diretrizes de Segurança da Informação

6.1. Adoção de Comportamento Seguro

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da Sociedade e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;
b) 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, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
c) Todo tipo de acesso aos dados e informações da Sociedade, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;
d) Assuntos relacionados ao desempenho de atividades e funções na Sociedade não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);
e) As senhas de acesso do Colaborador aos sistemas da Sociedade 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;
f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
g) Somente *softwares* homologados e previamente aprovados pela Sociedade podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe de serviços de informática da Sociedade;
h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da Sociedade;
i) 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;

j) Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Sociedade sem a autorização prévia do superior hierárquico do Colaborador; e

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Sociedade. 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 que possa colocar a Sociedade em risco.

6.2. Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela Sociedade 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 Sociedade, 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 Sociedade 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 do usuário aos sistemas;
b) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
c) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a "Política de Segregação das Atividades";
d) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Sociedade, ou que tenham mudado de função, se for o caso; e
e) Revisão periódica das autorizações concedidas.

6.3. Utilização da Internet

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da Sociedade, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

6.4. Monitoração e Controle

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Sociedade 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, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pela Área de Gestão de Riscos e de *Compliance* e/ou por prestador de serviços externo.

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 Sociedade, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

6.5. Sites na Internet

O acesso à sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da Sociedade. Adicionalmente, a Área de Gestão de Riscos e de *Compliance* poderá ser informada sobre acessos e tentativas de acesso à determinados sites.

6.6. Ramais Telefônicos

Os ramais telefônicos utilizados na sede da Sociedade pelos Colaboradores da Área de Gestão e da Área Comercial são gravados, e o conteúdo das conversas são armazenados em arquivos nos servidores da Sociedade. A Área de Gestão de Riscos e de *Compliance* possui livre acesso as gravações com o propósito de verificação de conteúdo.

Ao término da verificação, a Área de Gestão de Riscos e de *Compliance* emitirá termo de monitoramento, nos termos do Anexo I, informando o arquivo acessado, a data do acesso e se foram identificados indícios que possam indicar eventual infração ao disposto nesta Política, e nos demais documentos internos da Sociedade.

6.7. Telefones Celulares

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da Sociedade. Os aparelhos deverão ser mantidos no modo “silencioso” e somente poderão ser atendidas ligações pessoais de reconhecida importância.

6.8. Mensagens Instantâneas

A comunicação por mensagens instantâneas de texto e voz pela Internet deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da Sociedade.

6.9. Utilização e Conexão de Equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Sociedade.

A utilização de equipamentos pessoais nas instalações da Sociedade e a conexão destes na rede interna e à Internet requer autorização prévia e expressa da Área de Gestão de Riscos e de *Compliance*.

A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Área de Gestão de Riscos e de *Compliance.*

7. Segregação de Atividades

A Sociedade tem por objetivo o exercício da atividade de Gestão de Fundos e de Carteiras.

O Diretor Responsável pela Gestão de Fundos e de Carteiras ("Diretor Responsável") não pode ser responsável, direta ou indiretamente, por nenhuma outra atividade nos mercados financeiros.

Caso a Sociedade tenha interesse em desenvolver qualquer outra atividade nos mercados financeiros, essa atividade deverá, previamente ao seu início, ser submetida à apreciação dos diretores estatutários da Sociedade ("Diretoria") em reunião colegiada, ordinária ou extraordinária, ("Reunião de Diretoria") e aprovada pela maioria simples dos presentes, considerando votos individuais.

Se a nova atividade for aprovada, deverá ser segregada das atividades atualmente objeto da Sociedade. Atividades que não tenham sido aprovadas em Reunião de Diretoria serão consideradas estranhas à Sociedade.

7.1. Barreiras de Acesso à Informação

Os Colaboradores detentores de Informações Sigilosas, em decorrência de seu cargo e/ou função na Sociedade ou em outra entidade, devem estabelecer barreiras de acesso as Informações Sigilosas com os demais Colaboradores cujo acesso seja dispensável. A Área de Gestão de Riscos e de *Compliance* deve, quando necessário, manter o registro

dos Colaboradores que detenham Informações Sigilosas, com a indicação da Informação Sigilosa detida.

Essas barreiras servem para atender a diversos propósitos, incluindo:

a) A conformidade com leis e normas que governam o tratamento e a utilização de certos tipos de dados e/ou informação, em especial àquelas que podem ser caracterizadas como Informações Sigilosas;
b) Evitar situações que possam suscitar um provável Conflito de Interesses; e
c) Coibir a má utilização.

Via de regra, a Sociedade deverá manter barreiras de acesso à Informações Sigilosas em meio físico e eletrônico adequadas e necessárias à consecução de suas atividades

8. Endereço Eletrônico

Em cumprimento ao art. 14, II, da Instrução CVM nº 558/15, a presente Política está disponível no endereço eletrônico da Sociedade: http://www.adamcapital.com.br/.

Eventuais comunicações para a Área de Gestão de Riscos e de *Compliance* devem ser enviadas para: compliance@adamcapital.com.br

9. Revisões e Atualizações

Esta Política será revisada ao menos uma vez a cada semestre calendário. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

A Área de Gestão de Riscos e de *Compliance* informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Sociedade na Internet, conforme indicado acima.

10. Vigência

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação 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*.

Anexo I

TERMO DE MONITORAMENTO DE GRAVAÇÕES TELEFÔNICAS

Nesta data, _____, foi acessado o arquivo _____ contendo as gravações telefônicas efetuadas pelo ramal _____ e [não] foram identificados indícios que possam indicar eventual infração ao disposto na Política de Segurança das Informações e nas demais políticas internas da Adam Capital Gestão de Recursos Ltda.

[Data]

[Assinatura]