FLÓRIDA
INVESTIMENTOS

Política e Segurança da Informação

FLÓRIDA
INVESTIMENTOS

Sumário

1. Objetivo

Esta política estabelece princípios e diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações para que sejam mantidas integras e sem modificações indevidas, o acesso as informações são de conhecimento exclusivo de pessoas autorizadas, que fazem parte da estrutura da empresa, bem como descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

2. Alcance

Esta Política é extensiva a todos os empregados, colaboradores e prestadores de serviços da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS que fazem uso de sua infraestrutura de serviços e de seus sistemas informatizados.

3. Princípios

A informação é um ativo que possui grande valor, devendo ser adequadamente utilizada e protegida contra ameaças e riscos.

A informação pode ser manipulada de diversas formas tais como: por meio de arquivos eletrônicos, mensagens eletrônicas, Internet, banco de dados, em meio impresso, verbalmente, em mídias de áudio e vídeo etc.

A FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS visando garantir a segurança de suas informações, riscos de falhas, danos e/ou prejuízos que possam comprometer a sua imagem e seus objetivos, implantou políticas e procedimentos de segurança da informação que não é restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplicasse a todos os aspectos de proteção relacionada à tecnologia, procedimentos e pessoas.

São definidas 10 (dez) diretrizes básicas a serem seguidas;

I - O comprometimento com a melhoria contínua dos procedimentos relacionados com a Segurança da Informação;

II - As informações da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS, seus colaboradores, seus clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

III - A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

IV - Toda informação deve ser classificada conforme o nível de risco que ela representa, bem como, o nível de confidencialidade que ela requer, assegurado pelo Termo de Confidencialidade assinado por todo colaborador, em linha com o que prevê o Código de Ética;

V - O acesso às informações e recursos só deve ser feito, se devidamente autorizado;

VI - A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

VII - A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno

desempenho de suas atividades, ou seja, o acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do colaborador;

VIII - A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

IX

X - Será realizado, pelo menos uma vez ao ano, treinamento e conscientização sobre segurança de informação para todos colaboradores;

XI - Os riscos às informações da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS devem ser reportados à área de Compliance.

Essas diretrizes são todas embasadas conforme o art13° da ART:

I - Propiciar o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, profissionais e terceiros contratados;

II - Assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico; e

III - Implantar e manter treinamento para os seus sócios, diretores, alta administração e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e participem do processo de decisão de investimento.

4. Diretrizes

Somente atividades lícitas, éticas e autorizadas devem ser realizadas pelos funcionários, colaboradores e prestadores de serviços, quando da utilização dos recursos de processamento da informação da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS em consonância com as seguintes diretrizes:

O comprometimento com a melhoria contínua dos procedimentos relacionados com a Segurança da Informação.

5. Divulgação e Conscientização

A política deve ser divulgada, conhecida e cumprida por todos que utilizam recursos da informação de propriedade ou controlados pela FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS, sendo de responsabilidade de cada um, o seu fiel cumprimento.

A FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS disponibiliza aos sócios, diretores, colaboradores, durante o ano, treinamentos periódicos sobre segurança da informação com o objetivo de conscientizá-los sobre confidencialidade das informações, cyber segurança, engenharia social, phishing, entre outras potenciais ameaças à integridade dos sistemas de informação, além de guias sobre essas ameaças e de como se proteger delas e responder a elas.

Uma efetiva política de segurança da informação depende da conscientização de todos os envolvidos e do esforço constante para que se faça bom uso da informação e dos recursos de tecnologia existentes na FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS.

Todo funcionário, colaborador ou prestador de serviço que utilize os recursos de Tecnologia da Informação deve assinar “Termo de Compromisso e Responsabilidade” sobre o uso de ativos da informação.

6. Comportamento Seguro

É fundamental que os profissionais adotem comportamento seguro e compatível com os objetivos de proteção e a salvaguarda das informações da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS.

Os Diretores, Supervisores, funcionários e prestadores de serviços devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS.

Os colaboradores da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.

Todo tipo de acesso à informação da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS que não for explicitamente autorizado é proibido.

7. Confidencialidade

O Diretor de Compliance e Risco será o único responsável pela obtenção das informações relativas a análises de investimentos provenientes da empresa contratada pela FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS. Tais informações não serão compartilhadas por nenhuma outra pessoa –

Membro ou não -, nem mesmo pela Equipe Compliance, o que impossibilita a utilização destas informações por pessoas não habilitadas em processo de decisão de investimento.

Não obstante o acima descrito, a informação alcançada em função da atividade profissional desempenhada na FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS não pode ser transmitida de forma alguma a terceiros não-Membros ou a Membros não autorizados. Incluem-se aqui, por exemplo, posições compradas ou vendidas, estratégias e conselhos de investimento ou de desinvestimento, relatórios, análises e opiniões sobre ativos financeiros, dados a respeito de resultados financeiros antes da publicação dos balanços e balancetes da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS e dos fundos cujas carteiras sejam geridas pela FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS, transações efetuadas e que ainda não foram publicadas, informações oriundas de estudos efetuados pelas áreas da sociedade.

8. Controle de Acesso a Informações

Todo acesso a diretórios e sistemas de informações da Ultra deve ser controlado pela área de Compliance.

Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pelo Diretor de Compliance.

O controle do acesso a sistemas de informações da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil;

- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora;

- Os Colaboradores devem evitar circular em ambientes externos à FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do Investidor, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;

- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;

- As informações que possibilitem a identificação de um Investidor da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS ou do próprio Investidor;

- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc;

- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;

- A senha de acesso do Colaborador ao sistema da Ultra é pessoal e intransferível; e

- O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de Compliance sempre que necessário.

9. Cópia de Segurança

Todas as informações do servidor da FLÓRIDA INVESTIMENTOS & GESTÃO DE RECURSOS, do banco de dados dos clientes etc. são enviadas para o servidor. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com backup.

10. Segurança Cibernética

A Política de Segurança Cibernética tem como objetivo estabelecer as regras, procedimentos e controles para aprimorar a segurança cibernética da Gestora, devendo ser cumprida por todos os seus Colaboradores, independentemente de seu nível hierárquico ou função, bem como funcionários ou terceiros, mediante o planejamento de ações necessárias para manter a segurança, confidencialidade, integridade e disponibilidade dos dados e sistemas de informação utilizados através de métodos de prevenção e detecção de vulnerabilidades mitigando assim os acidentes relacionados com o ambiente cibernético.

A Política segue práticas de mercado, regulamentação e autorregulação aplicáveis, incluindo o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e o Guia de Cibersegurança da ANBIMA.