Política de Confidencialidade e Segurança da Informação

Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da JOURNEY CAPITAL.

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a JOURNEY CAPITAL (doravante, "Colaboradores").

Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao responsável por *Compliance*, a quem caberá avaliá-las e submetê-las ao Comitê de *Compliance* ou ao Conselho de Ética, que tomará as medidas cabíveis.

O responsável pelo *Compliance* deve garantir o atendimento a esta Política.

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, em função de mudanças legais/regulatórias.

Definições

São consideradas informações confidenciais aquelas não disponíveis ao público, que:

- ✓ **Identifiquem dados pessoais, patrimoniais ou estratégicos;**
- ✓ **Sejam objeto de acordo de confidencialidade celebrado com terceiros;**

- ✓ **Identifiquem ações estratégicas – dos negócios da empresa, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão dos negócios, clientes e fundos, ou reduzir sua vantagem competitiva; e que**
- ✓ **O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.**

Não caracteriza descumprimento desta Política a divulgação de informações confidenciais em atendimento a ordens do Poder Judiciário ou autoridade administrativa ou legislativa, seja em âmbito municipal, estadual ou municipal, bem como, quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na JOURNEY CAPITAL:

Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando ele for de fato necessário;

Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da JOURNEY CAPITAL:

- ✓ As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- ✓ A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;
- ✓ A concessão de acessos às informações confidenciais 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;

- ✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- ✓ Segregação de instalações, equipamentos e informações comuns, quando aplicável;
- ✓ A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao responsável pelo *Compliance*.

A JOURNEY CAPITAL apenas coletará dados pessoais e sensíveis para o estrito atendimento da regulação em vigor. A JOURNEY CAPITAL mantém constante revisão dos seus procedimentos e controles internos de modo a cumprir eficientemente com a regulação vigente, inclusive os requerimentos da Lei Geral de Proteção de Dados ("LGPD").

Processos e Controles

Para assegurar que as informações sejam adequadamente protegidas, a JOURNEY CAPITAL definiu os seguintes processos/controles:

Identificação da Informação

O Colaborador que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

Classificação da Informação

Algumas informações podem ser classificadas como Confidencial.

Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Controles para informações classificadas como "Confidencial"

O acesso às informações confidenciais deve ser controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento e descarte.

O Colaborador responsável pela informação gerada deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte.

O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista. Ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

Gestão de Acessos

Os equipamentos, ferramentas e sistemas concedidos aos colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à JOURNEY CAPITAL.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da JOURNEY CAPITAL, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas ao *Compliance*, que poderá ou não conceder a exceção.

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de Segurança da Informação devem ser reportados ao Responsável pelo *Compliance*, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Testes de Controles

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes.

Um plano de teste deve ser efetuado pelo responsável por *Compliance* verificando se:

- ✓ **Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;**
- ✓ **Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;**
- ✓ **Há segregação física e lógica;**
- ✓ **Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;**
- ✓ **A manutenção de registros permite a realização de auditorias e inspeções.**

Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à JOURNEY CAPITAL não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

Rastreamento

É permitido o uso pessoal dos equipamentos de informática e de comunicação utilizados pelos Colaboradores para a realização das atividades profissionais. Lembrando que, como tais recursos (e-mails, sistemas, computadores, telefones etc.) pertencem à JOURNEY CAPITAL, estes são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria e/ou exigência judicial.

Termo de Conhecimento

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com a Política de Segurança da Informação.

Os Colaboradores que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento devem solicitar ao *Compliance* eventuais dúvidas e esclarecimentos sobre o tema de Segurança de Informação.

Anexo I

Termo de Conhecimento da

POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

NOME		
ÁREA	*CARGO*	
DOC. IDENTIDADE No	*TIPO*	*CPF*

Declaro que tenho conhecimento da Política de Confidencialidade e Segurança da Informação da JOURNEY CAPITAL, e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) **adotar e cumprir as diretrizes indicadas na Política;**

b) **comunicar imediatamente ao responsável por *Compliance* qualquer violação desta Política de que eu venha a ter conhecimento, independente de qualquer juízo individual, materialidade ou relevância da violação.**

Estou ciente e concordo que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo termo, bem como, em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____ (local)

_____

Assinatura do Colaborador