POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Sumário

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Introdução

A Política de Segurança da Informação da Kobold Gestora de Fundos Ltda (“Kobold”), aplica-se a todos os sócios, colaboradores, prestadores de serviços, clientes e parceiros de negócio, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Kobold, ou ainda que acessem informações a ela pertencentes.

Todo e qualquer usuário de recursos computadorizados inseridos no ecossistema de negócios da nossa instituição tem por responsabilidade zelar, proteger e reportar incidentes referentes a segurança ou integridade das informações e dos equipamentos e plataformas de tecnologia da Kobold.

Objetivos

A Política de Segurança da Informação da Kobold visa proteger as informações de propriedade e/ou sob guarda da Kobold, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Kobold, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas a esta instituição.

Qualquer informação sobre a Kobold ou de qualquer natureza relativa às atividades da empresa e a seus sócios, prestadores de serviços, clientes e parceiros de negócio, obtida em decorrência do desempenho das atividades normais do colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance, assim definido no Código de Ética e Conduta da Kobold.

Segurança da Informação

As medidas de segurança da informação utilizadas pela Kobold têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É terminantemente proibido que os colaboradores, prestadores de serviços ou parceiros de negócio façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Kobold e circulem em ambientes externos à empresa com os mesmos, sem prévia autorização do Diretor de Compliance. Isso porque tais arquivos contêm informações que são consideradas 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 Kobold. Nestes casos, quem 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, nas dependências da Kobold, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

Adicionalmente, os colaboradores devem se abster de utilizar pen-drives, HD externo ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Kobold.

A rede da Kobold é separada logicamente em 3 instâncias, com graus distintos de controle de acesso, baseados no grau de sensibilidade de cada uma:

- Acesso: composta pelo ponto de acesso sem fio (wifi) do escritório, roteadores e firewall. Essa rede é acessível por meio de senha de rede. Existe uma separação da rede de acesso corporativa, de uso exclusivo de colaboradores e da rede de acesso de visitantes;

- Serviço de email e arquivos: SaaS que oferece de maneira integrada e online a gestão de usuários do domínio Kobold, de seus emails e arquivos. Esse serviços são acessados de qualquer lugar, com controle de acesso individualizado por usuário, senha e MFA;

- Servidores de aplicação: rede virtualizada em provedor de serviços de nuvem. É acessível apenas para usuários selecionados, que têm necessidade de atuar de forma direta na manutenção de servidores e da aplicação, mediante uso de VPN e controle individual de usuário e senha.

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

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Kobold.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia dos sócios. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos.

Todo conteúdo que está na rede pode ser acessado pelo Diretor de Compliance caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais ou administrativas.

Lei Geral de Proteção de Dados

A Kobold realiza tratamento de dados pessoais de diversas formas e por diversos aspectos, para diversas das finalidades previstas nos termos da Lei nº Lei 13.709/18 (“LGPD”). Dentre eles, se destaca a coleta de dados de clientes, colaboradores e visitantes, por meio de comunicação por e-mail, registro na recepção e

contratações, dentre outras formas de coleta de dados pessoais.

Desta forma, a Kobold é considerada controladora de dados pessoais, nos termos do artigo 5º, inciso VI da LGPD, isto é, uma pessoa jurídica, de direito privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Por sua vez, seus colaboradores com acesso a dados pessoais, de terceiros ou não, são considerados operadores de dados pessoais, nos termos do artigo 5º, inciso VII da LGPD: pessoas naturais, de direito privado, que realizam o tratamento de dados pessoais em nome do controlador.

Assim, a Kobold utiliza o Código de Ética e Conduta em conjunto com o instrumento particular de confidencialidade e outras disposições, para regular e orientar seus colaboradores quanto aos seus direitos e deveres de proteção de dados pessoais, enquanto colaboradores da Kobold.

Sistemas e Backups

Todos os dados da Kobold são protegidos por sistemas automatizados de Backup. Eles são feitos diariamente, de maneira automática, ao início e fim do horário comercial, e permanecem em disponibilidade rápida por 30 (trinta) dias. Após esse período, são arquivados e permanecem disponíveis, mas arecuperação poderá levar algumas horas. Diariamente, um backup anterior é restaurado para garantir a acessibilidade da informação, caso seja necessário. Essas informações são retidas por um período de 10 anos, podendo ser removidas apó sesse período.

O ambiente no qual os sistemas são executados é em nuvem, o acesso a ele é limitado aos colaboradores de Tecnologia, através de acessos individuais e monitorados. Todo ambiente é criado a partir de um documento executável, aplicado automaticamente sempre que uma mudança se faz necessária, através de um acesso específico e monitorado. Toda mudança na infraestrutura é revisada e aprovada por, pelo menos, mais uma pessoa além do autor da mudança, além de gravada e salva em nova versão com uma justificativa da necessidade da mudança e todas as alterações necessárias no ambiente em nuvem.

O acesso à informação de clientes, pelos colaboradores, é pessoal e intransferível. Ele é limitado às atividades pertinentes ao colaborador.

Segregação de Atividades

A segregação das atividades de administração de carteira de valores mobiliários tem por objetivo evitar que ocorram diversos problemas de conflito de interesses e uso indevido de informações privilegiadas, bem como o de criar os procedimentos e controles que permitam uma maior qualidade do serviço.

A Kobold reconhece que a segregação das atividades é um requisito essencial para o efetivo cumprimento de suas estratégias de administração de recursos de terceiros, uma vez que cumpre um papel importantíssimo na defesa dos interesses de seus clientes.

Logo, a Kobold segrega suas diversas áreas a partir dos procedimentos operacionais por elas adotados e cada um de seus funcionários possui microcomputador, usuário com perfil de acesso ao ambiente computacionale telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro funcionário.

O acesso a informações é restrito aos empregados que delas necessitem para exercerem suas funções, na exata medida que isto for necessário, a critério do Diretor Responsável (“Pessoas Autorizadas”). Isto também

se reflete nos sistemas de gerenciamento da informação, onde cada usuário tem uma amplitude de acesso limitada e que permite o controle do que é acessado, por quem e quando é acessado, vide art. 4, §8º, da Resolução CVM n.º 21/21.

Ademais, cada colaborador possui um código de usuário e e-mail.

A rede de computadores da Kobold permite a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores da empresa que garantem áreas de armazenamento de dados distintas no servidor com controle de acesso por usuário. Cada colaborador tem à disposição uma pasta de acesso exclusivo, garantindo que só o usuário tenha acesso aos documentos de sua responsabilidade.

A Kobold acredita que as medidas acima relacionadas sejam eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, estando sempre em busca de servir adequadamente aos seus clientes e cumprir com suas obrigações fiduciárias.

Vigência e Atualização

Esta política será revisada periodicamente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo.

Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.