POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Avenida Angélica, nº. 2346, Conjunto 161 B - Consolação - CEP 01228-200 - São Paulo – SP
Tel.: 11 3512.5400 - Fax: 11 4800-5400

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 acesse 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 referente 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 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, clientes, 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 informações 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.

É proibida a conexão de equipamentos na rede da Kobold que não estejam previamente autorizados.

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 também 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.

Sistemas e Backups

Todos os dados da Kobold são protegidos por sistemas automatizados de Backup realizados diariamente que garantem a recuperação rápida do ambiente. Para servidores que possuem atualizações de informação diárias, o backup é feito diariamente em fitas LTO5, já para os servidores que possuem atualizações programadas ou apenas quando necessário, os backups são feitos nos finais de semana também em fitas LTO5. Existe também uma rotina diária para backup do servidor de arquivos do ambiente, este backup por sua vez é realizado em uma unidade D2D (HP StoreOnce). Para o banco de dados, a regra é de 2 backups Full diários, uma para o D2D e outra para NAS e backups diferenciais a cada meia hora para o NAS e a cada 1 hora para o D2D. A Kobold possui rotinas diárias de backup do seu ambiente com arquivamento diário (4 dias), semanal (8 semanas) e mensal (12 meses). Os back-ups dos servidores são feitos como imagem (máquina virtual) a fim de ter um RTO pequeno. As fitas são armazenadas dentro do próprio Data Center.

De forma a preservar os sistemas e informações da Kobold, acesso ao Data Center é realizado apenas por funcionários autorizados pela área de infraestrutura da Kobold.

A Kobold adota procedimentos internos que visam garantir a confidencialidade e integridade das informações corporativas. A rede da Kobold não é acessada sem autorização da equipe de infra-estrutura de TI, os e-mails são guardados por 10 anos com estrutura na nuvem.

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 criar os procedimentos e controle que permitirão uma maior qualidade do serviço.

A Kobold reconhece que a segregação das atividades é um requisito essencial para o efetivo cumprimento às 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 ela adotados e cada funcionário da Kobold possui seu próprio microcomputador, usuário com perfil de acesso ao ambiente computacional e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro funcionário.

Ainda nesse sentido acesso a informações relativas à administração de recursos de terceiros é restrito aos empregados que necessitem desta informação para exercerem suas funções na exata medida que isto for necessário, a critério do Diretor Responsável (“Pessoas Autorizadas”). Isto também se refletirá nos sistemas de gerenciamento da informação, nos quais cada usuário terá uma amplitude de acesso limitada e que permitirá o controle do que é acessado, por quem e quando é acessado, vide art. 4, §8º, da Instrução CVM n.º 558/15.

Ademais, cada colaborador possui um código de usuário e email. Ainda, 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 própria de acesso exclusivo, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade.

Sendo assim, a Kobold acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, estando sempre em busca de servir adequadamente 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.