MUITO ALÉM DE UMA SIMPLES **MUDANÇA**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 2.2

ABRIL 2024

Comitê de Sustentabilidade e ASG

Escopo da Empresa

A One Moving é uma empresa de mudanças reconhecida mundialmente. Fornecemos serviços de mudança internacional, nacional e armazenagem de alta qualidade aos nossos clientes. Temos nossos galpões e caminhões em Caieiras e escritório em São Paulo. A empresa é familiar desde 2016. **Esta política abrange todos os nossos sites.**

Galpões: Rua José Lopes, 284, Pq. Industrial Araucária, Caieiras – São Paulo – SP, CEP: 07747-150

Escritório: Av. das Nações Unidas, 12901 – 6° andar – Torre Oeste – Brooklin, São Paulo – SP, CEP: 04578-000

Política de Segurança da Informação

OBJETIVO

Consolidar os princípios e as práticas de governança corporativa adotados pela One Moving e o seu compromisso com a adoção das melhores práticas de governança corporativa, tendo como referência o Código das Melhores Práticas de Governança Corporativa.

A Política de Gestão e Governança adotado pela One Moving tem como princípios direcionadores a transparência, a equidade, a prestação de contas (accountability) e a responsabilidade corporativa, os quais, quando convertidos em práticas de governança corporativa, permitem o aperfeiçoamento da gestão, a harmonização de interesses, a sustentabilidade do negócio e a geração de valor para a perenidade da Companhia.

Os 4 pilares da Gestão e Governança são Anticorrupção (suborno, conflito de interesse, lavagem de dinheiro e fraude), Práticas Anticompetitivas (manipulação de lances, fixação de preços, preços predatórios e dumping e alocação de território), Gestão Responsável da Informação (segurança da informação e gerenciamento e conformidade com diretrizes e regulamentos globais) e Compras Sustentáveis

Em seu código de Ética, a empresa exige que todos os colaboradores conduzam suas operações, seus projetos e seus serviços em conformidade com as leis e regulamentos de mercado, sem prejuízo ao equilíbrio natural.

ABRANGÊNCIA

Todos os funcionários, colaboradores, clientes, usuários, parceiros ou fornecedores da One Moving.

VIGÊNCIA

Esta política entrará em vigor na data da sua publicação.

Política de Segurança da Informação

DEFINIÇÕES

- **Informação:** É a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;
- **Segurança da Informação:** É o conjunto de ações e controles que tem como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos empresa;
- **Confidencialidade:** A informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;
- **Integridade:** Salvaguarda da exatidão da informação e dos métodos de processamento;
- **Disponibilidade:** As pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes sempre que necessário;
- **Conformidade:** Processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores, etc.) e com aspectos legais e regulatórios relacionados à administração da empresa, dentro de princípios éticos e de conduta estabelecidos pela One Moving;
- **Incidente de Segurança da Informação:** Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;
- **Risco de Segurança da Informação:** Riscos associados à violação da confidencialidade e integridade, bem como da disponibilidade das informações da companhia nos meios físicos e digitais.

Política de Segurança da Informação

GESTÃO DE SEGURANÇA CIBERNÉTICA

- ***Gestão de Riscos*** *- Nossa abordagem para gerenciar riscos cibernéticos começa com o entendimento de que a segurança é responsabilidade de todos. Realizamos reuniões regulares de avaliação de riscos onde identificamos quais informações são vitais para nossa operação e onde elas podem estar vulneráveis. A partir daí, trabalhamos para fortalecer essas áreas, sempre priorizando as ameaças que poderiam causar o maior dano.*

- ***Configuração Segura*** *- Para assegurar que nossos sistemas estejam sempre configurados de forma segura, mantemos uma política de 'menor privilégio' e desabilitamos serviços que não são necessários, reduzindo assim a superfície de ataque. Todos os sistemas são regularmente atualizados para garantir que quaisquer brechas de segurança sejam corrigidas assim que descobertas.*

- ***Trabalho em Casa e Móvel*** *- Implementamos soluções como VPNs seguras e autenticação de dois fatores para manter nossas conexões seguras e nossos dados protegidos, mesmo em redes não confiáveis.*

- ***Gestão de Incidentes*** *- Se um incidente de segurança ocorrer, temos planos prontos para agir rapidamente e minimizar o impacto. Nossos backups regulares garantem que podemos restaurar dados perdidos com pouco tempo de inatividade, e aprendemos com cada incidente para melhorar constantemente nossas práticas.*

- ***Prevenção de Malware*** *- Utilizamos softwares antimalware de ponta e mantemos esses sistemas sempre atualizados. Além disso, realizamos campanhas de conscientização para que todos possam reconhecer sinais de tentativas de ataques, como phishing, ajudando a evitar que malwares comprometam nossos sistemas.*

Política de Segurança da Informação

GESTÃO DE SEGURANÇA CIBERNÉTICA

- ***Gerenciando o Acesso do Usuário*** *- Cada membro da equipe tem acesso apenas às informações necessárias para realizar seu trabalho. Isso é controlado por sistemas de gestão de identidade e acesso, que são revisados regularmente para assegurar que todos os acessos estão corretos e seguros.*

- ***Monitoramento*** *- Monitoramos constantemente a atividade em nossas redes, o que nos permite detectar e responder a ameaças em tempo real. Nossas equipes estão sempre alerta, garantindo que possíveis problemas sejam identificados antes que causem danos.*

- ***Segurança da Rede*** *- Protegemos nossa infraestrutura de rede com múltiplas camadas de segurança, incluindo firewalls modernos e sistemas de detecção de intrusão. Essas medidas nos ajudam a evitar acessos não autorizados e proteger nossos dados e serviços críticos.*

- ***Controles de Mídia Removível*** *- Entendemos os riscos associados ao uso de dispositivos removíveis e temos políticas estritas para seu uso. Todos os dispositivos são criptografados e monitorados para garantir que informações sensíveis sejam protegidas, tanto dentro quanto fora da empresa.*

- ***Responsabilização, Educação e Conscientização do Usuário*** *- Promovemos uma cultura de segurança através de treinamentos regulares e comunicados. Todos os usuários são alertados quanto a mensagens ou arquivos de origem duvidosas, e repassam essas informações para o responsável de segurança para avaliar se há riscos em prosseguir com a abertura desses itens. É vital para nós que todos entendam sua parte na proteção da nossa empresa.*

Política de Segurança da Informação

DIRETRIZES

- **Informação é Patrimônio:** Toda informação gerada, adquirida, manuseada, armazenada, transportada e/ou descartada nas dependências e/ou em ativos da empresa é considerada patrimônio da empresa e deve ser utilizada exclusivamente para os interesses corporativos.
- **A Responsabilidade e o comprometimento devem ser de todos:** Todos os colaboradores, estagiários, terceiros, fornecedores e parceiros, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, tanto com a One Moving, como de seus clientes, parceiros e fornecedores, dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.
- **O acesso à informação deve ser gerenciado:** O acesso lógico, o controle de acesso físico e o uso da informação da One Moving devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.
- **Incidentes de Segurança precisam ser tratados:** Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos da One Moving.
- **Os ativos da One Moving e sua utilização podem ser monitorados:** A One Moving pode monitorar o acesso e a utilização de seus ativos tecnológicos, como dos ambientes, equipamentos e sistemas da informação, de forma que ações indesejáveis ou não autorizadas sejam detectadas.
- **Auditoria de conformidade com as práticas de SI:** A One Moving pode auditar periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus colaboradores, estagiários, terceiros, fornecedores e parceiros em relação ao estabelecido nesta Política e na legislação aplicável.

Política de Segurança da Informação

PAPÉIS E RESPONSABILIDADES

- **Área de TI -** Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na One Moving, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano. *Designamos um Gestor de Segurança da Informação que é o principal responsável por todos os aspectos da segurança cibernética em nossa empresa. Essa pessoa tem a autoridade e os recursos necessários para manter, atualizar e implementar as políticas de segurança, garantindo que estejam alinhadas com as melhores práticas do setor e com os objetivos estratégicos da nossa organização.*

- **Colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas da One Moving -** Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da One Moving; Informar as situações que comprometam a segurança das informações nas unidades organizacionais da One Moving. Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente a One Moving, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal; Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares); Garantir que os requisitos de Segurança da Informação constem nas aquisições e/ou implementações tecnológicas.

Política de Segurança da Informação

PAPÉIS E RESPONSABILIDADES

- ***Treinamento, Atualização e Divulgação*** *- Nossa equipe de segurança cibernética, liderada pelo CISO, monitora continuamente a eficácia dos nossos procedimentos de segurança através de auditorias regulares, testes de penetração e acompanhamento das mais recentes ameaças cibernéticas. Realizamos revisões anuais para avaliar e, se necessário, atualizar nossas políticas e práticas de segurança. Essas revisões são fundamentais para garantir que continuamos resilientes contra novas ameaças e vulnerabilidades. Um programa de conscientização, educação e treinamento em Segurança da Informação é disponibilizado para garantia dos objetivos, princípios e diretrizes definidas nesta Política. O programa deve ser seguido adequando-se às necessidades e responsabilidades específicas de cada colaborador, estagiário, terceiro, fornecedor e parceiro da One Moving.*

Política de Segurança da Informação

CORREIO ELETRÔNICO

O objetivo desta política é informar aos colaboradores da One Moving quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do One Moving é para fins corporativos e relacionados às atividades do colaborador dentro da empresa.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico para:

- enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente vulnerável a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Produzir, transmitir ou divulgar mensagem que:
  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da One Moving;
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha arquivos com código executável (.com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - vise obter acesso não autorizado a outro computador, servidor ou rede;
  - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - vise burlar qualquer sistema de segurança;

Política de Segurança da Informação

- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico poderão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Função
- Telefone(s)
- Correio eletrônico
- Logo da empresa
- Slogan da empresa

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da One Moving, cabendo a cada um utilizá-los e manuseá-los e conservá-los corretamente no uso exclusivo de suas atividades de trabalho.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um responsável de TI da One Moving, ou de quem este determinar.

Política de Segurança da Informação

O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de TI da One Moving.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida aprovação da área de TI da One Moving.

É proibido o armazenamento de arquivos pessoais e/ou não pertinentes ao negócio do One Moving (fotos, músicas, vídeos, etc..). Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os colaboradores devem informar a área de TI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela área de TI da One Moving ou por terceiros devidamente contratados para o serviço.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela One Moving, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

Política de Segurança da Informação

- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.
- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

INTERNET

A política visa o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a One Moving e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

Política de Segurança da Informação

SENHAS

Os usuários que não possuem perfil de administrador são recomendáveis ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível. Já os usuários que possuem perfil de administrador ou acesso privilegiado são recomendáveis utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o RH deverá imediatamente comunicar tal fato a área de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

O administrador poderá ter acesso aos equipamentos dos colaboradores, exceto as senhas dos mesmos.

Política de Segurança da Informação

BACKUP

Regulamentar a política de backup das informações eletrônicas, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento, visando garantir a segurança, integridade e disponibilidade dos dados.

TIPOS DE BACKUPS:

- Backup: Cópia de segurança de informações consideradas importantes para o negócio.
- Backup Completo: Cópia de segurança de todos os dados selecionados para terem uma salvaguarda de informação.
- Backup Incremental: Somente os arquivos novos ou modificados desde o último backup são transmitidos.

Os colaboradores responsáveis pela gestão dos backups deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

DESCARTE DE MÍDIA E PAPÉIS

Informação somente pode ser descartada depois de devido processo e autorização. Mídias somente podem ser descartadas se a informação armazenada puder ser descartada ou tiver sido preservada em outro meio.

Portanto, o descarte de mídias deve compreender os métodos de controle de classificação de documentos que permitam identificar mídias contendo informações sensíveis, de maneira que sejam guardadas e destruídas de maneira segura, e a Instrução de descarte para mídia;

Em caso de papel, devem ser usadas fragmentadoras de papel, podendo ser fragmentado manualmente, sendo também possível destruir cartões magnéticos

Política de Gestão e Governança

CONSIDERAÇÕES

- ✓ Esta política está alinhada às demais políticas da One Moving.
- ✓ As exceções, eventuais violações e casos omissos a esta Política devem ser submetidos à apreciação do Comitê de Sustentabilidade e ASG e encaminhados para posterior aprovação pelos órgãos competentes.
- ✓ Esta política pode ser desdobrada em outros documentos normativos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.
- ✓ É de responsabilidade do Comitê de Sustentabilidade e ASG garantir que esta política seja de conhecimento de todos os colaboradores das áreas envolvidas, através de treinamentos e informes, utilizando-se as ferramentas de comunicação que forem necessárias.
- ✓ Esta política deve ser revisada sempre que necessário e mediante a realidade da One Moving.
- ✓ Esta política deverá seguir e respeitar todas as diretrizes da Lei Geral de Proteção de Dados – Lei nº 13.709/2018, e as normas internas a ela vinculada.

Sanções

Atitudes que violem das leis e políticas de segurança da informação são puníveis para pessoas físicas e, se a empresa for considerada parte da violação, a empresa pode ser multada gravemente, ser excluída de licitações de contratos públicos e sofrer danos à sua reputação.

Ponto de Contato

Se você não tiver certeza se algo está violando alguma lei ou política de segurança da informação, pergunte ao seu gestor ou envie um e-mail para o Comitê de Sustentabilidade e ASG em **compliance@onemoving.com.br** para aconselhamento e orientação.

Comitê de Sustentabilidade e ASG

Wesley Thomé
CEO One Moving

Rodrigo Vicente
CFO
One Moving

Roberto Xavier
Gerente de Qualidade
One Moving

André Alemi
Diretor de Coordenação
One Moving

Rubia Moreira
Gestora de RH
One Moving

Rogério Pagano
Diretor de Operações
One Moving Portugal

Joaquim Thomé
CEO
Grupo EP&A

CONTROLE DE DOCUMENTAÇÃO

VERSÃO	EDIÇÃO	ELABORADO POR	DATA	REVISADO POR	DATA
2	1	RODRIGO VICENTE	FEV/23	COMITE DE SUSTENTABILIDADE E ASG	FEV/23
2	2	RODRIGO VICENTE	ABR/24	COMITE DE SUSTENTABILIDADE E ASG	ABR/24