POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política, inspirada na Legislação vigente e nos valores praticados pela AMF Import Comércio e Locação de Veículos Ltda. (“AMF Import”), denominada “Política de Segurança da Informação”, dispõe sobre as regras de Segurança da Informação e ações e controles para garantir a preservação dos aspectos de confidencialidade da AMF Import.

Mensagem do CEO

Joaquim Thomé

> “ *Temos que nos desafiar a entrar de verdade em uma trilha de autoconhecimento. A transformação interna de cada indivíduo é o primeiro passo para causarmos a mudança que queremos ver no mundo. Por isso, é necessário sermos conscientes, estarmos preparados e termos atitudes coerentes aos nossos discursos.* ”

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ABRANGÊNCIA

Todas as pessoas físicas e jurídicas que se relacionam, direta ou indiretamente, com a AMF Import (“Todos”).

VALIDADE

Esta Política permanecerá em vigor por prazo indeterminado.

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 integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos;
- 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;
- 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.

DIRETRIZES

- Informação é patrimônio: Toda informação gerada, adquirida, manuseada,

armazenada, transportada e/ou descartada nas dependências e/ou em ativos da AMF Import é considerada patrimônio e deve ser utilizada exclusivamente para os interesses corporativos;

- A responsabilidade e o comprometimento devem ser de Todos: Todos são responsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, tanto com os da AMF Import, como de clientes, 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 AMF Import 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;
- Os ativos da AMF Import e sua utilização podem ser monitorados: A AMF Import 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 Segurança da Informação: A AMF

Import pode auditar periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de Todos em relação ao estabelecido nesta Política e na legislação aplicável.

RESPONSABILIDADES

- Área de TI:
  - Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na AMF Import, promovendo ações de interesse, programas educacionais e de conscientização do capital humano.
- Colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas:
  - Conhecer e cumprir as normas e orientações estabelecidas nesta Política e legislação que compõem a presente Política;
  - Informar as situações que comprometam a segurança das informações nas unidades organizacionais;
  - Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo e aplicativos comerciais utilizados deve ser tratada como de propriedade da AMF Import, não devendo ser considerada como pessoal, particular ou

confidencial, mesmo que arquivadas em pasta ou computador 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.

- Treinamento, Atualização e Divulgação:
  - 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 Todos.
- A área de Segurança da Informação atua em alinhamento com os princípios de gestão de riscos ocupacionais previstos na NR-1, colaborando com a integridade do ambiente de trabalho e com a mitigação de riscos que possam comprometer a saúde e segurança das pessoas.

CORREIO ELETRÔNICO (E-MAIL CORPORATIVO) E APLICATIVOS COMERCIAIS

O uso do correio eletrônico e de aplicativos comerciais é para fins corporativos e relacionados às atividades de cada um dentro da AMF Import.

É proibido o uso do correio eletrônico e de aplicativos comerciais para:

- Enviar mensagens pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico/aplicativo comercial 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 AMF Import;
  - 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;

- 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 como 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 e de aplicativo comercial, se autorizada a utilização desses meios, poderão incluir assinatura com o seguinte formato:
  - Nome;
  - Função/Cargo;
  - Telefone(s);
  - Logo da AMF Import.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos e ferramentas disponibilizados são de propriedade da AMF Import, 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 AMF Import, ou de quem este determinar.

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

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 AMF Import.

É proibido o armazenamento de arquivos pessoais e/ou não pertinentes ao negócio da AMF Import (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 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 usuários 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 ou por terceiros devidamente contratados para o serviço;
- O usuário deverá manter a configuração do equipamento disponibilizado, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas, assumindo a responsabilidade como custodiante de informações;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos usuários, datas e horários de acesso;
- Proibido tentar ou obter acesso não autorizado a outro computador, servidor

ou rede;

- Proibido burlar quaisquer sistemas de segurança;
- Proibido acessar informações confidenciais sem explícita autorização do proprietário;
- Proibido interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Proibido 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;
- Proibido hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Proibido utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

INTERNET

Esta Política de Segurança da Informação 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 uma pessoa, a responsabilidade perante a AMF Import e a legislação será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

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 tenham 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 possui acesso integral e sem limitação aos equipamentos e ferramentas disponibilizadas.

BACKUP

- 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 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.

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.

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

SANÇÕES

Toda e qualquer atitude/ato que viole a presente Política pode ser punível, nos termos da lei, pela Diretoria.

Colaboradores e prestadores que comprovadamente infringirem a presente Política, sem prejuízos das demais penas previstas na legislação e nos respectivos contratos, estão sujeitos às seguintes penalidades independentes:

- Advertência escrita;
- Suspensão;
- Demissão/Rescisão por justa causa.

Parceiros comerciais e fornecedores que comprovadamente infringirem a presente Política, sem prejuízos das demais penas previstas na legislação e nos respectivos contratos, estão sujeitos às seguintes penalidades independentes:

- Suspensão de atividades;
- Cancelamento do Contrato.

CONTATO DO DATA PROTECTION OFFICER - DPO

A AMF Import disponibiliza o contato do seu Data Protection Officer - DPO, Sr.

Alexandre Julião Santos Silva, através do e-mail dpo@grupoepea.com.br, como canal seguro e direto para receber comunicações. Todas as informações serão tratadas de forma sigilosa e garantimos confidencialidade do declarante em todos os casos de denúncias, bem como a não retaliação para aqueles que denunciarem.

CONSIDERAÇÕES FINAIS

Esta Política está alinhada às demais políticas da AMF Import.

Eventuais exceções, violações e casos omissos a esta Política devem ser submetidos à apreciação do respectivo Comitê e encaminhados para posterior aprovação pela Diretoria.

Esta Política pode ser desdobrada em outros documentos normativos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidas.

A AMF Import se reserva no direito de revisar, modificar e revogar a presente “Política de Segurança da Informação”, a qualquer tempo e formato, sem necessidade de aviso prévio. Qualquer revisão e modificação refletirão as alterações legais e/ou introduzidas nas práticas em matéria de Segurança da Informação.

AMF IMPORT