POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de segurança da informação, no EXPRESSO PRINCESA DOS CAMPOS, aplica-se a todos os funcionários, prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento de dados da companhia, ou acessem informações pertencentes à EXPRESSO PRINCESA DOS CAMPOS. Todo e qualquer usuário que utilize recursos computadorizados da companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- Exponha a companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações, ou ainda da perda de equipamento.

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio do EXPRESSO PRINCESA DOS CAMPOS.

É DEVER DE TODOS

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a companhia e deve sempre ser tratada profissionalmente.

CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do líder de cada área estabelecer critérios relativos ao nível de confidencialidade da informação gerada por sua área de acordo com a relação abaixo:

1 – Pública
2 – Interna
3 – Confidencial
4 – Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

PROGRAMAS ILEGAIS

Não é permitida a instalação de software nos equipamentos da companhia. Todo equipamento disponibilizado para a utilização dos colaboradores da companhia contém apenas softwares profissionais que servem para a execução da sua rotina de trabalho diária.

PERMISSÕES E SENHAS

Para o acesso a rede da companhia todo usuário deverá possuir um login e senha previamente cadastrados pela TI. Cada gestor quando possuir necessidade de que seus colaboradores tenham acesso a rede, deve abrir chamado na TI. A qual providenciara o acesso através da Ficha de Acesso por setor.

COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de dados de qualquer tipo (pessoais, ou profissionais) através de dispositivos móveis (pendrive, celulares, etc.), não é permitido o compartilhamento de dados de qualquer tipo através de pastas compartilhadas na rede, e não é permitido o compartilhamento de dados através de e-mail particular ou recursos de *cloud computer*. Todos os dados de utilização profissional devem ser armazenados na unidade U e compartilhados quando necessário através da unidade P:.
Em caso de extrema necessidade do compartilhamento dos dados citados acima em local de armazenamento diferente da unidade U: ou P: deve ser comunicado a área de TI.

CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

O armazenamento de dados no computador ou dispositivo de informática que não seja na unidade U da rede de computadores do EXPRESSO PRINCESA DOS CAMPOS não possuirá recurso de cópia de segurança (*Backup*), ficando estes sobre responsabilidade do próprio usuário que armazenou em local não seguro.

DOCUMENTOS PESSOAIS

É proibida a utilização de qualquer dispositivo de TI da companhia para armazenamento de documentos, fotos, vídeos, ou qualquer outro documento pessoal.
Caso seja localizado qualquer tipo de arquivos citados acima , serão deletados imediatamente e o colaborador receberá medida administrativa.

ACESSO INTERNET

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais no EXPRESSO PRINCESA DOS CAMPOS abertura de chamado citado no item Permissões e Senhas. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.
É proibido o acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da companhia;
- Que promovam discussão pública sobre os negócios da companhia;
- Que possibilitem a distribuição de informações de nível “Confidencial”;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

USO DO CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico fornecido pelo EXPRESSO PRINCESA DOS CAMPOS é um instrumento de comunicação interna e externa para a realização do negócio. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem e não podem ser contrárias à legislação vigente e nem aos princípios éticos do EXPRESSO PRINCESA DOS CAMPOS.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Expressões que indicam preconceito de raça, cor, etc.;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da companhia;
- Um usuário não poderá utilizar e-mail de outro usuário.

Não será permitido o uso de e-mail pessoal para a troca de informações ou de arquivos profissionais do EXPRESSO PRINCESA DOS CAMPOS.

USO DE NOTEBOOK E CELULAR NO EXPRESSO PRINCESA DOS CAMPOS

Os usuários que tiverem direito ao uso de notebook, celular ou qualquer outro equipamento de propriedade do EXPRESSO PRINCESA DOS CAMPOS, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- Não é permitido alterações nas configurações do equipamento recebido.
- Em caso de furto, deverá ser registrada uma ocorrência em uma delegacia de policia e enviar uma cópia para a TI da companhia, bem como informar imediatamente o seu superior imediato.

USO DE ANTIVÍRUS

Todas as estações de trabalho deverão possuir antivírus instalado. Nenhum usuário pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado

Ponta Grossa, 03 de abril de 2017.