POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
(modelo)

A Política de segurança da informação, na A EMPRESA, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à A EMPRESA.

Todo e qualquer usuário de 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.***

Missão do Setor de Informática:

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

Objetivo da Política de Segurança da Informação:

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da A EMPRESA.

É Dever de todos dentro da A EMPRESA:

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

01 – CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela 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.

02 – DADOS PESSOAIS DE FUNCIONÁRIOS

A A EMPRESA se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários alem daqueles relevantes na condução do seu negócio.
Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais.
Dados Pessoais de Funcionários sob a responsabilidade da A EMPRESA não serão usados para fins diferentes daqueles para os quais foram coletados.
Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da A EMPRESA.

03 – PROGRAMAS ILEGAIS

É terminantemente proibido o uso de programas ilegais (PIRATAS) na A EMPRESA. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da Companhia.
Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

04 – PERMISSÕES E SENHAS

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias.
Por segurança, a Informática recomenda que as senhas tenham sempre um mínimo de 8 (oito) caracteres alfanuméricos.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc) deverão comunicar ao Setor de Informática qual será o seu substituto quando de sua ausência da A EMPRESA, para que as permissões possam ser alteradas (delegação de poderes).

05 – COMPARTILHAMENTO DE PASTAS E DADOS

É de obrigação dos usuários rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

06 – CÓPIA DE SEGURANÇA (BACKUP) DO SISTEMA INTEGRADO E SERVIDORES DE REDE

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da Informática e deverão ser feitas diariamente.
Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado. Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando, que o referido mês foi encerrado.
Nos meses pares, a Informática enviará 1 (uma) cópia extra da fita do "backup" de fechamento do referido mês, para ser arquivada na Contabilidade.

07 – SEGURANÇA E INTEGRIDADE DO BANCO DE DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

08 – ADMISSÃO/DEMISSÃO DE FUNCIONÁRIOS/TEMPORÁRIOS/ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da Companhia deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Companhia. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.
Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.
No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.
Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da A EMPRESA.
Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

09 – TRANSFERÊNCIA DE FUNCIONÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

10 – CÓPIAS DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da A EMPRESA.
No caso das informações consideradas de fundamental importância para a continuidade dos negócios da A EMPRESA o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

11 – PROPRIEDADE INTELECTUAL

É de propriedade da A EMPRESA, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a A EMPRESA.

12 – USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na A EMPRESA. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.
O uso da Internet será monitorado pelo Setor de Informática, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.
A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da Companhia, com base em recomendação do Supervisor de Informática.
Não é permitido instalar programas provenientes da Internet nos microcomputadores da A EMPRESA, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.
Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados 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 A EMPRESA;
- Que promovam discussão pública sobre os negócios da A EMPRESA, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

13 – USO DO CORREIO ELETRÔNICO – ("e-mail")

O correio eletrônico fornecido pela A EMPRESA é um instrumento de comunicação interna e externa para a realização do negócio da A EMPRESA.
As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da A EMPRESA, não podem ser contrárias à legislação vigente e nem aos princípios éticos da A EMPRESA.
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;
- 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 A EMPRESA.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.
Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.
Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da A EMPRESA.
O Setor de Informática poderá, visando evitar a entrada de vírus na A EMPRESA, bloquear o recebimento de e-mails provenientes de sites gratuitos.

14 – NECESSIDADES DE NOVOS SISTEMAS , APLICATIVOS E/OU EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da A EMPRESA em relação a definição de compra e substituição de "software" e "hardware".
Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.
Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

15 – USO DE COMPUTADORES PESSOAIS (LAP TOP) DE PROPIEDADE DA A EMPRESA

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da A EMPRESA, 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.
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

16 – RESPONSABILIDADES DOS GERENTES/SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.
-

17 – SISTEMA DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da A EMPRESA, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da A EMPRESA.
Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

18 – USO DE ANTI-VÍRUS

Todo arquivo em mídia proveniente de entidade externa a A EMPRESA deve ser verificado por programa antivírus.
Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.
Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.
O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

19 – 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.

Rio de Janeiro, 08 de Agosto de 2006.

Presidente

Diretor Vice Presidente Adm./Financeiro

Supervisor de Informática·

*Nome:*_____

*Número:*_____

_____

Funcionário