POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SET MANUTENÇÕES

Este documento foi elaborado pelo DTI - Departamento de Tecnologia da Informação e contêm as normas para utilização da rede de comunicação, ativos de informática e acesso à Internet. Destina-se aos colaboradores, em seus diversos aspectos, apresentar normas para utilização dos recursos, de forma a preservar o patrimônio e a informação, no que se refere aos Departamentos computacionais de comunicação.

1. Objetivos

Esta política tem como objetivo garantir a correta e adequada utilização da Internet, Intranet, Extranet, Ativos de Informática e Recursos de Computação e Comunicação. Visa, de forma geral, a proteção do ambiente tecnológico, sua abrangência estende-se a todos os colaboradores diretos ou indiretos desta empresa, que utilizam os recursos de rede, comunicação e informação.

A SET MANUTENÇÕES se exime das responsabilidades decorrentes da violação de qualquer um dos itens deste documento. Fica o colaborador responsável pelos atos ilícitos ou danosos, praticados utilizando os recursos computacionais da Instituição, que venham a causar prejuízos ou ônus às informações, sistemas, imagem, equipamentos da Instituição ou terceiros. Os colaboradores devem estar cientes de que as informações geradas e manuseadas a partir dos sistemas da SET MANUTENÇÕES são de propriedade da mesma.

Ressalta-se que, primordialmente, todos os colaboradores que necessitem ter acesso aos recursos de rede, comunicação e informação deverão, como requisito básico, assinar o “Termo de Responsabilidade”. Neste, o colaborador se compromete à estrita observância e obediência às condições e requisitos básicos para o acesso aos recursos computacionais da empresa. O descumprimento incorrerá nas penalidades cabíveis, de acordo com a infração cometida e com legislação vigente.

As atitudes consideradas violação a esta política estão descritas na seção 2 e encontram-se divididas nas seguintes categorias:

I. Utilização dos Ativos de Informática;

II. Utilização da Rede;

III. Utilização da Internet, Intranet e Extranet;

IV. Utilização do e-mail institucional;

V. Utilização de equipamentos particulares;

VI. Adição de Recursos;

VII. Utilização de Senhas;

As normas elencadas trazem como premissa básica, o conceito de que tudo o que não for explicitamente permitido é considerado violação à Política de Segurança da Informação. Salienta-se que, em virtude de ser a segurança da informação um processo contínuo, novas normas e possíveis alterações nesta política serão implementadas. Neste último caso,revoga-se automaticamente a política anterior. Todos os colaboradores, que fazem uso dos recursos computacionais da empresa devem manter-se atualizados e obedientes às normas em vigor. Este documento estará disponível no quadro de aviso de todos campos de atuação.

2. POLÍTICA

2.1 Utilização dos Ativos de Informática

Esse tópico visa definir as normas de utilização dos ativos de informática da empresa

I Uso dos Computadores

- Os Desktops / Notebooks da SET MANUTENÇÕES são identificados pela TAG e vinculados a cada usuário, que será responsável por todas as atividades realizadas no equipamento.
- Sempre bloqueie a tela ou faça logout ao se ausentar do computador.
- É proibido instalar ou utilizar softwares/hardwares não autorizados pelo Deptº de Tecnologia da Informação (T.I.).
- Não armazene arquivos pessoais (fotos, músicas, filmes, etc.) nos computadores.
- Arquivos corporativos devem ser salvos somente no armazenamento do dispositivo para preservar sua integridade e acessibilidade.
- Reparos nos computadores são estritamente proibidos.

Apenas softwares licenciados e homologados podem ser instalados.

É vedado ao colaborador:

a. Instalar ou remover softwares nos computadores da empresa sem prévia autorização;

b. Abrir computadores ou outros ativos de informática para qualquer tipo de reparo. Cabe ao colaborador de tais ativos notificar o Deptº de TI quando qualquer problema for identificado;

c. Alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar

qualquermodificação que possa causar algum problema futuro;

d. Retirar ou transportar qualquer equipamento da empresa sem autorização prévia do Deptº de TI e Patrimônio;

e. Instalar, desinstalar, desabilitar ou alterar qualquer software ou hardware a fim de tornar omesmo total ou parcialmente inoperante;

f. Retirar ou desconectar qualquer equipamento da rede sem um motivo aceitável;

g. Comprometer, por mau uso ou de forma intencional, equipamento pertencente a empresa;

h. Autorizar, sem devido conhecimento e liberação do Deptº de TI, a utilização de equipamentos de informática por pessoas sem vínculo com a instituição;

i. Utilizar equipamentos e informações para outros fins, que não sejam atividades ligadas à instituição;

j. Retirar/danificar licenças/placas identificadoras de patrimônio afixadas nos equipamentos de informática ou travas/lacres de segurança disponível em tais;

k. Conectar e/ou configurar equipamento à rede, sem a prévia liberação do Deptº de TI;

l. Alterar, excluir ou inutilizar informações ou meios de acesso a aplicativos/equipamentos de forma indevida ou sem prévia autorização;

m. Apropriar-se de segredos da empresa ou colaboradores, pertencentes à Instituição através de qualquer meio, eletrônico ou não, sem prévia autorização do proprietário de tais informações;

n. Tornar vulnerável a segurança dos ativos de informática portáteis (notebook, data show, pen drive, etc);

o. Compartilhar arquivos ou diretórios sem prévia autorização do Deptº de TI;

II. Utilização da Rede

Esse tópico visa definir as normas de utilização da rede da empresa

É vedado ao colaborador:

a. Tentar ou obter acesso não autorizado a qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conexão a servidor ou

conta, cujo acesso não seja expressamente autorizado ao usuário;

b. Tentar colocar à prova a segurança da rede ou de equipamentos de informática, tanto da Instituição quanto de terceiros;

c. Conectar dispositivos não autorizados na rede local, equipamentos de rede sem fio, equipamentos que permitam a ligação da rede da instituição à outra rede, que interfiram na frequência/trabalho de operação dos equipamentos da instituição ou que forneçam serviços de rede, como protocolos DHCP, NAT ou outros;

d. Realizar testes de rede ou estabelecer conexões ad hoc em local onde há o alcance da rede da empresa;

e. Tentar interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo negação de serviço (DoS – ataque cibernético que visa tornar um serviço ou um computador indisponível para usuário legítimo), congestionamento em redes, tentativas de sobrecarregar um servidor ou "quebrar" (invadir) um servidor;

f. Infringir a privacidade de qualquer usuário;

g. Monitorar, interceptar, interromper, modificar servidores, computadores, arquivos ou sistemas de computação instalados dentro da Instituição ou efetuar o mascaramento/falsificação/personificação de endereços/contas de *login* com objetivo de ocultar-se dos sistemas de segurança da Instituição;

h. Configurar manualmente o endereço IP de computadores particulares ou pertencentes à instituição. A distribuição de endereços de rede é feita pelo serviço de DHCP, mantido e disponível na empresa pelo Deptº de TI;

i. Conectar computador particular na rede da Instituição sem a devida assinatura do “Termode Responsabilidade” e autorização do Deptº de TI ;

j. Criar, obter ou divulgar imagens, vídeos, documentos ou arquivos com conteúdo abusivo, ofensivo, difamatório, discriminatório, pornográfico, obsceno, injurioso, vexatório, enganoso, calunioso, violento, vulgar, de propaganda não solicitada, de assédio, ameaça,de uso de falsa identidade, ou que seja contrário às normas éticas atuais;

k. Utilizar-se de outro sistema de *proxy* que não seja o determinado pelo Deptº de TI;

2.1 Uso da Rede

- É proibida qualquer tentativa de acesso não autorizado aos recursos tecnológicos.

- Alterações nas configurações de rede e na inicialização das máquinas não são permitidas.
- Não há suporte técnico para dispositivos pessoais.
- Conteúdo pornográfico, discriminatório ou inadequado não pode ser acessado, armazenado ou editado na rede.
- Jogos e outros softwares não autorizados não podem ser instalados.
- Arquivos só podem ser criados ou removidos dentro da área designada ao usuário.

Acesso a pastas e compartilhamentos de departamentos será concedido apenas mediante necessidade.

III. Utilização da Internet, Intranet e Extranet

Esse tópico visa definir as normas de utilização da Internet, Intranet e Extranet da empresa.

3.1. Uso da Internet

- É proibido acessar sites com conteúdo pornográfico, racista, relacionado a drogas, comércio eletrônico, classificados, jogos, bate-papos ou serviços de streaming.
- Downloads de arquivos suspeitos ou que comprometam a segurança da rede são vetados.
- Redes sociais e sites de relacionamento, como Facebook e Instagram, estão bloqueados, salvo exceções previamente autorizadas.
- Para liberação de sites específicos, é necessário abrir o chamado no HELPDESK com justificativa.
- A divulgação de informações confidenciais em grupos de discussão, listas ou bate-papos é proibida e passível de sanções

É vedado ao colaborador:

a. Divulgar, acessar, reter ou disseminar material que não esteja de acordo com as normas, atividades ou políticas da Instituição por meio dos recursos computacionais disponibilizados na Instituição;
b. Utilizar recursos disponíveis para: armazenamento, distribuição ou execução de qualquer tipo de arquivo ou software não autorizado pelo Deptº de TI;

c. Utilizar ferramentas de compartilhamento de arquivos tais como: ***Torrent, Morpheus, Kazaa, e-mule, Ares e similares;***
d. Utilizar a Internet ou Intranet para jogos individuais ou contra oponentes;

e. Utilizar programas P2P, ou qualquer outro similar, para efetuar *download/upload;*

f. Acessar serviços de *streaming* de rádio utilizando os recursos computacionais disponíveis;

g. Utilizar e/ou divulgar parâmetros/configurações/*so*ftwares, impedindo o bom funcionamento dos ativos de informática ou burlar os sistemas de segurança a fim de conseguir acesso ou privilégios indevidos;

h. Utilizar ou propagar softwares mal-intencionados, como vírus, vermes, cavalos de tróia, *keyloggers*, ou programas que controlem outros computadores (Back Oriffice, Netbus ou similares) através dos recursos disponibilizados pela empresa;

i. Divulgar informações confidenciais da empresa através meios eletrônicos ou não;

j. Apropriar-se ou distribuir, por intermédio de qualquer meio físico ou virtual de softwares licenciados ou licenças de software de propriedade exclusiva da instituição bem como qualquer informação, sem autorização por escrito;

k. Utilizar os recursos disponibilizados pela instituição para distribuir cópia de qualquer material protegido por direitos autorais, propriedades intelectuais, leis, regulamentações similares, patentes ou outras normas/políticas;

l. Tentar ou obter acesso a recursos computacionais com o nome de usuário de outra pessoa;

m. Divulgar, por intermédio dos equipamentos de informática disponibilizados para uso, informações que possam causar alguma forma de dano físico ou moral a terceiros;

n. Utilizar procedimentos ou recursos com a finalidade de obter informações que trafegam pela rede da empresa;

o. Causar falhas nos recursos computacionais da instituição, ou por intermédio destes em outras redes, através da transmissão de arquivos ou outras informações;

p. Utilizar a personificação, mascarando endereços de computadores de rede, e-mail ou logins ocultando a própria identidade e/ou responsabilizar terceiros por qualquer tipo de ação;

q. Comprometer ou excluir informações ou arquivos, que não sejam de sua propriedade, armazenados nos recursos computacionais da Instituição sem autorização;

r. Utilizar os recursos computacionais disponibilizados para realizar o envio de mensagens idênticas a grande quantidade de destinatários (SPAM) ou enviar grande quantidade de mensagens a um destinatário (*Mail Bombing*);

s. Efetuar o *download* (baixa) de programas de entretenimento, filmes ou jogos;

IV. Utilização do e-mail Institucional

a. O e-mail institucional deve ser de uso restrito para as atividades relacionadas ao desempenho das funções do colaborador;
b. É de responsabilidade do usuário todas as mensagens transmitidas sob seu nome de usuário;

c. Para manter o bom funcionamento do sistema de e-mail o STI poderá efetuar bloqueio dee-mails com arquivos de código executável como (.vbs, .hta, .src, .cpl, .reg, .dll, .inf, exe,
.com, .bat, .pif, .js) ou outras extensões usualmente utilizadas por vírus, e-mails para domínios ou destinatários que afetem negativamente os ativos de informática ou exponha a instituição a riscos de segurança;

d. A conta de e-mail dos ex-colaboradores da empresa será desativada após 10 dias do desligamento da instituição;

É vedado ao colaborador:

e. Perturbar colaborares ou outras pessoas através do envio frequente de mensagens ou envio de mensagens muito grandes;

f. Tentar ou obter acesso a conta de e-mail de outra pessoa;

g. Utilizar o e-mail institucional para enviar mensagens idênticas a grande quantidade de destinatários (SPAM) ou enviar grande quantidade de mensagens a um destinatário (*Mail Bombing*). Isso inclui, qualquer tipo de mala direta, como anúncios ou publicidades que não condizem com as atividades institucionais. Ressalva-se, neste caso, que fica preservado o direito de envio de e-mail para todos os colaboradores por parte da Instituição, quando se fizer necessário;

h. Propagar mensagens em cadeia ou “pirâmides”, independentemente da vontade do destinatário de receber tais mensagens;

i. Sobrecarregar um servidor, usuário ou site com o envio de e-mails muito extensos ou compostos por múltiplas partes;

j. Modificar qualquer informação do cabeçalho do remetente;

k. Utilizar apelidos, nomes falsos ou ocultar-se a fim de enviar algum e-mail;

l. Divulgar informações que possam causar danos físicos, materiais ou morais a terceiros;

V Utilização de equipamentos particulares

Esse tópico visa definir as normas de utilização de equipamentos particulares nas dependências da empresa.

a. O uso de equipamentos de informática particular, só será permitido após aprovação da Diretoria;
b. As informações, arquivos e softwares contidos no equipamento são responsabilidadesde seu portador/proprietário;
c. Cabe ao portador do equipamento manter um *firewall* pessoal ativo e um antivírus atualizado e em execução, não sendo possível ao portador responsabilizar a instituição por qualquer problema causado por invasão ou pragas virtuais;

d. Ao utilizar a rede de dados e comunicação da instituição, o portador deve seguir as mesmas regras de utilização da rede, Internet e Intranet;

VI Adição de Recursos

É vedada aos usuários da rede a adição de quaisquer recursos, sejam eles microcomputadores, impressoras, ou outros equipamentos. A adição de novos equipamentos por parte do usuário deve ser solicitada por comunicação interna e deverá ser aprovada pelo Deptº de TI. Todos os equipamentos ligados à rede devem obedecer a padrões de instalação, de designação de endereços e domínio, portanto, uma vez aprovada a solicitação, será realizada a adição do equipamento pelo Deptº de TI. A adição de recursos à revelia da empresa compromete a administração e a segurança da rede, assim como a assistência aos equipamentos/dispositivos.

VII Uso de senhas

Esse tópico visa definir as normas de utilização de senhas utilizadas para acesso a serviços,sites ou computadores da SET MANUTENÇÕES.

a. É dever do colaborador manter o sigilo das suas senhas de acesso à rede e aos sistemas, bem como, seguir as recomendações de segurança de como se criar uma senha forte;

b. Toda ação efetuada com a utilização do usuário e senha do colaborador é de estrita responsabilidade do dono da senha, não podendo este responsabilizar outras pessoas;

c. Regra para criação de senhas fortes: utilizar no mínimo oito caracteres, onde a mesma deve ser composta por letras (maiúsculas e minúsculas), números e

caracteres especiais(*,^,%,$,#, entre outros). A senha deve ser alterada a cada 270 dias e ser diferente, pelo menos, das cinco últimas senhas utilizadas;

Importante sobre as senhas

- Senhas NÃO podem ser alteradas.
- Administradores de sistemas (TI) são responsáveis pela criação e alteração de senhas.
- Usuários devem garantir a segurança de suas credenciais, que são pessoais e intransferíveis.

VIII Lei Geral de Proteção de Dados (LGPD)

As informações acessadas durante as atividades na SET MANUTENÇÕES devem ser tratadas com confidencialidade, em conformidade com a LGPD (Lei nº 13.709/2018), que regula o uso e proteção de dados pessoais no Brasil.

Bruno Miguel Queiros Esteves Marques

Diretor da SET MANUTENÇÕES

Elaborado por: Departamento de Informática TI

Aprovado por: Diretor

Revisão: 001	Ano de Criação: 2019	Data da Revisão: 17/02/25