Data da Atualização	Responsável	Versão
21.12.2024	Diretor de Compliance e PLD	5

CONTEA CAPITAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Data da Atualização	Responsável	Versão
21.12.2024	Diretor de Compliance e PLD	5

1. Introdução

A presente política tem por objetivo estabelecer normas técnicas para a utilização dos recursos tecnológicos disponíveis na empresa e disponibilizado a seus colaboradores e prestadores de serviço para o desempenho de suas funções e atividades profissionais.

Tais normas são fornecidas a título de orientação do funcionário. Em caso de dúvida sobre o que é considerado, de alguma forma, violação, o usuário deverá enviar previamente um e-mail para administracao@conteacapital.com.br visando esclarecimentos e segurança.

Nos termos da Política de Utilização da Rede, a empresa procederá o bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com o aqui estabelecido ou de forma prejudicial à Rede.

Denominam-se recursos tecnológicos os seguintes recursos e serviços abaixo descriminados:

a) Hardware: Componente ou conjunto de componentes físicos de um computador ou de seus periféricos;
b) Software: Conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas, bem como os dados a eles associados, empregados durante a utilização do sistema;
c) Internet: Conjunto de computadores interligados em uma rede de abrangência mundial, que se comunicam utilizando o protocolo TCP/IP;
d) Intranet: Conjunto de computadores e outros equipamentos de uma instituição que formam uma rede utilizando o protocolo TCP/IP e são ligados à Internet usualmente através de um sistema de proteção (Firewall);
e) Extranet: Conjunto de mecanismos capazes de prover níveis específicos de acesso a dados e sistemas pertencentes à intranet de uma determinada instituição a pessoas que estejam acessando estes sistemas a partir da Intranet;
f) Correio eletrônico: Serviço que possibilita a troca assíncrona e ubíqua de mensagens através de recursos da Internet;

g) Sítio da Internet também conhecido como site: Conjunto de documentos apresentados ou disponibilizados na rede mundial (web) por um indivíduo, empresa ou instituição, que pode ser acessado em um endereço específico da rede Internet (URL – Uniform Resource Locator), podendo ser subdividido em páginas com endereços específicos e próprios;

h) Bancos de dados: Qualquer arquivo estruturado de dados, acessível segundo determinados critérios, que seja centralizado, descentralizado ou distribuído de modo funcional ou geográfico;

i) Suporte: Assessoria prestada por pessoal especializado visando solucionar problemas e imperfeições em sistemas e equipamentos de informática;

j) Certificação digital: conjunto de técnicas criptográficas que permitem verificar a autenticidade, autoria e integridade de um documento em formato digital;

k) Download: Obtenção de cópia, em máquina local, de um arquivo originalmente armazenado em máquina remota ou em rede.

2. Utilização da Rede

Esse tópico visa definir as normas de utilização da rede sua identificação de acesso, armazenamento e manutenção de dados nos servidores e tentativas não autorizadas de acesso à rede de dados ou informações nela contidas.

Não são permitidas tentativas de obter acesso não autorizado, tais como fraudar ou utilizar a autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

Não é permitida tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.

Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários.

Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/logoff da rede ou bloqueio do desktop através de senha.

Todos os usuários são responsáveis pela manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis.

Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos tecnológicos da empresa.

Não é permitido criar, armazenar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme abaixo:

Diretório C: (usuário) Arquivos Pessoais inerentes à empresa

Diretório D: (departamento) Arquivos do departamento em que trabalha

Diretório D: (público) Arquivos temporários ou de compartilhamento geral

Em alguns casos podem haver mais de um compartilhamento referente aos arquivos do departamento a qual se faz parte.

A pasta PÚBLICO ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível.

É obrigatório armazenar os arquivos inerentes a empresa no servidor de arquivos para garantir o backup dos mesmos.

É proibida a instalação ou remoção de programas que não forem devidamente acompanhadas pelo responsável por TI ou pelos sócios executivos.

É vedado a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento técnico.

Não será permitido a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

3. Utilização de E-Mail

Objetivo: Estabelecer as diretrizes para a utilização de correio eletrônico, englobando as atividades de envio, recebimento, estabelecimento de cotas de armazenamento, gerenciamento das contas e auditoria.

É proibido o assédio ou perturbação de usuários de correio eletrônico, sejam estes internos ou externos à empresa, considerando-se a linguagem utilizada, frequência ou tamanho das mensagens.

É proibido o envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail.

É proibido o envio de grande quantidade de mensagens de e-mail ("junk mail" ou "spam"); isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, propaganda política, correntes entre outros avisos de caráter ou origem duvidosas.

É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides".

É proibido o envio de mensagens eletrônicas mal-intencionadas, tais como "mail-bombing" ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail.

É proibido o envio de mensagens eletrônicas com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

É proibido o envio de mensagens eletrônicas para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

É proibido forjar qualquer das informações do cabeçalho do remetente.

É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.

4. Utilização de acesso à Internet

Objetivo: Estabelecer as diretrizes de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

É proibido utilizar os recursos da empresa para fazer o download ou distribuição de programas ou dados não legalizados.

É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo passível de sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.

Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas.

Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização dos sócios executivos.

Caso a empresa julgue necessário haverá bloqueios de acesso à:

1. arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
2. domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

Não será permitido a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus e afins.

5. Verificação da utilização da Política de Utilização da Rede

Visando garantir as regras o cumprimento das normas mencionadas acima a empresa se reserva no direito de:

a) Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa;

b) Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
c) Instalar uma série de programas e equipamentos para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet;
d) Instalar autenticação de acesso em dois fatores (2FA) para acesso ao e-mail Contea;
e) Instalar sistema de segurança de Geolocalização onde ninguém com credenciais pode acessar nossa rede fora do Brasil; e
f) Instalar bitlocker em todas as máquinas, fornecendo segurança contra-ataques off line (caso nossos hd's / ssds sejam roubados e iniciados em outro dispositivo não conseguiram ter acesso às informações da máquina).

6. Política de backup

Diariamente, é realizada cópia de todos os dados armazenados no servidor. Caso haja necessidade, funcionários podem solicitar arquivos dos últimos sete dias à diretoria.

7. Acesso ao Servidor

No servidor da CONTEA CAPITAL, há espaço para armazenamento dos arquivos das mais diversas áreas. Exceto o drive D (público), todas as pastas do drive D têm acesso restrito, conforme a função do funcionário. Para liberação de acesso a diretórios, enviar a solicitação para administracao@conteacapital.com.br e tal solicitação será analisada pelos sócios executivos.

8. Das Punições

O não cumprimento pelo funcionário das normas ora estabelecidas neste documento (¨Políticas de Utilização da Rede¨), seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

a) Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada.
b) Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.
c) Desligamento da equipe: Fica desde já estabelecido que o sócio executivo, no uso do poder diretivo e disciplinar que lhe é atribuído, poderá aplicar a pena de desligamento, quando entender devida.