Política de uso aceitável de sistemas e equipamentos

Norma #	Vigência	Versão
09	01/11/2021	1.0

Contato	E-mail	Telefone
Lemuel Victor Dias	victor.dias@medicamental.com.br	(16) 3505-4900

Índice:

1 Visão geral

A intenção da empresa ao publicar uma Política de Uso Aceitável de Sistemas e Equipamentos não é impor restrições que sejam contrárias à cultura estabelecida de abertura, confiança e integridade da empresa.

A empresa está empenhada em proteger seus recursos, funcionários, parceiros, clientes e fornecedores de atos ilegais ou prejudiciais, realizados consciente ou inconscientemente.

Os sistemas e equipamentos fornecidos pela empresa, incluindo, mas não se limitando a servidores, desktops, notebooks, tablets, equipamentos de rede, telefones, smartphones, projetores, softwares, aplicativos, sistemas de negócio, banco de dados, mídia de armazenamento, etc., são de propriedade da empresa. Esses sistemas e equipamentos devem ser usados para fins comerciais apenas, atendendo aos interesses da empresa e de seus clientes no curso normal das operações.

A segurança efetiva é um esforço de equipe que envolve a participação e o suporte de todos os funcionários da empresa que lidam com informações e/ou

sistemas de informação. É responsabilidade de cada funcionário conhecer essas diretrizes e conduzir suas atividades de acordo com elas.

2 Objetivo

O objetivo desta política é descrever o uso aceitável de sistemas e equipamentos de informática na empresa.

Essas regras existem para proteger o funcionário, a empresa, seus clientes e fornecedores.

O uso impróprio de sistemas e equipamentos de informática expõe a empresa a riscos, incluindo ataques de vírus, comprometimento de sistemas e serviços de rede e questões legais.

3 Aplicabilidade

Esta norma se aplica:

- A todas as unidades, áreas, setores e departamentos da empresa.
- A todos os analistas de segurança da informação e administradores de sistemas responsáveis pela manutenção de sistemas, softwares, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela empresa.
- A todos os dirigentes, funcionários em tempo integral, funcionários em meio período, funcionários em tempo parcial, trabalhadores contratados, consultores, estagiários, trabalhadores temporários, prestadores de serviços, agentes, parceiros, fornecedores e usuários autorizados que acessam as dependências da empresa.

- A todos os sistemas, aplicativos, dispositivos e equipamentos de TI gerenciados pela empresa que armazenam, processam ou transmitem dados e informações, incluindo redes de computadores, hardwares, softwares e aplicativos, dispositivos móveis e sistemas de telecomunicações.

- A todas as informações utilizadas na empresa, em todos os formatos. Isso inclui informações processadas por outras organizações em suas relações comerciais com a empresa.

4 Norma

4.1 Obrigações

Existem vários responsáveis pelo uso adequado e aceitável de sistemas e equipamentos. Isso inclui responsabilidades da empresa e responsabilidades do usuário / funcionário. Cada uma delas é descrita nesta política.

4.1.1 Obrigações da empresa

É responsabilidade da empresa garantir que todos os equipamentos sejam mantidos atualizados e capazes de funcionar conforme necessário para atingir os objetivos da empresa.

Além disso, a empresa assume a responsabilidade pela instalação de aplicativos de antivírus/anti-malware e todos os aplicativos de linha de negócios considerados necessários para que os funcionários desempenhem as suas funções.

4.1.2 Obrigações do funcionário

É responsabilidade do funcionário que usa os sistemas, equipamentos e dispositivos da empresa garantir a operação segura destes, incluindo o uso correto e o manuseio cuidadoso do hardware físico.

Qualquer equipamento danificado, perdido ou roubado deve ser relatado ao departamento de TI imediatamente.

Cabe ao funcionário também garantir que softwares e aplicativos não pertencentes à organização não sejam instalados no hardware ou em outros equipamentos pertencentes à empresa. Tais instalações somente serão permitidas se expressamente autorizadas pela empresa. Em tais casos o funcionário deverá garantir que não se trata de software ou aplicativo pirata.

Para equipamentos de computação portátil, incluindo laptops, tablets e smartphones, o usuário do equipamento também deve considerar o acesso aos dados armazenados no dispositivo e as redes que podem estar disponíveis para o dispositivo se conectar.

Os funcionários não devem usar o equipamento de maneira que viole as leis ou regulamentos locais, estaduais ou federais.

4.1.3 Uso de equipamento da empresa para outras atividades

Os equipamentos fornecidos pela empresa devem ser usados no cumprimento das funções, tarefas diárias e responsabilidades do funcionário.

A empresa reconhece que pode haver momentos excepcionais em que o equipamento poderá vir a ser utilizado em outras atividades, mas espera que esse uso seja feito de forma limitada, segura e não recorrente. Não será permitido o uso consistente de equipamentos da empresa para atividades não relacionadas ao trabalho.

4.1.4. Armazenamento de dados, documentos e arquivos pessoais

Os recursos de armazenamento da empresa devem ser usados pelos funcionários no desempenho de suas funções.

Todos os arquivos de que os funcionários precisam para desempenhar suas funções poderão ser armazenados.

Outros arquivos considerados necessários pelo funcionário também poderão ser armazenados. É responsabilidade do funcionário “limpar” o espaço de

armazenamento dos equipamentos fornecidos pela empresa e garantir que arquivos que não pertençam a ele sejam removidos.

4.2. Uso geral e propriedade

As informações proprietárias da empresa que são armazenadas em dispositivos eletrônicos e de computação pertencentes ou alugados pela empresa, por funcionários ou terceiros, permanecem como propriedade exclusiva da empresa.

Cada funcionário deve garantir, por meios legais ou técnicos, que as informações proprietárias sejam protegidas de acordo com os padrões de Proteção de Dados adotados pela empresa.

Cada funcionário tem a responsabilidade de relatar imediatamente o roubo, perda ou divulgação não autorizada de informações proprietárias da empresa.

Cada funcionário poderá acessar, usar ou compartilhar informações proprietárias da empresa apenas na medida em que for autorizado e necessário para cumprir as suas funções atribuídas.

Os funcionários são responsáveis por exercer o bom senso quanto à razoabilidade do uso pessoal.

Para fins de segurança e manutenção de rede, indivíduos autorizados podem monitorar equipamentos, sistemas e tráfego de rede a qualquer momento, de acordo com as normas de segurança da informação implementadas pela empresa.

A empresa reserva-se o direito de auditar redes e sistemas periodicamente para garantir a conformidade com esta política.

4.3. Segurança e informações proprietárias

Todos os dispositivos móveis e de computação que se conectam à rede interna devem cumprir as normas de segurança da informação implementadas pela empresa.

As senhas de nível de sistema e de usuário devem estar em conformidade com a política de senhas estabelecida. É proibido fornecer acesso a outro indivíduo, seja deliberadamente ou por meio de falha em procedimentos destinados a proteger o acesso não autorizado.

Mensagens enviadas por funcionários de um endereço de e-mail da empresa para grupos de mídia devem conter a informação de isenção de responsabilidade declarando que as opiniões expressas são estritamente próprias e não necessariamente as da empresa, a menos que a mensagem seja para fins comerciais.

Os funcionários devem ter muito cuidado ao abrir anexos de e-mail recebidos de remetentes desconhecidos, que podem conter malware.

4.4. Uso aceitável de sistemas e equipamentos

Os funcionários que usam equipamentos da empresa (ou seus próprios equipamentos) estão representando a empresa dentro ou fora do horário comercial.

Os funcionários são responsáveis por garantir que este equipamento seja usado de maneira eficaz, correta, segura, ética e legal.

São exemplos de atividades aceitáveis:

- Acessar compartilhamentos de arquivos ou bancos de dados para trabalhar em material de propriedade da empresa do qual o funcionário precisa para desempenhar suas funções;
- Usar navegadores Web para obter informações comerciais de sites comerciais;
- Uso de e-mail para comunicação empresarial;
- Acessar informações de sistemas em um dispositivo móvel de propriedade da empresa;

- Impressão de documentos confidenciais para uma reunião de equipe.

4.5. Uso inaceitável de sistemas e equipamentos

Os funcionários não devem usar sistemas e equipamentos da empresa para fins ilegais, antiéticos, prejudiciais à empresa ou improdutivos, pois isso coloca a organização em risco.

Os funcionários podem ser isentos dessas restrições durante o curso de suas responsabilidades legítimas de trabalho (por exemplo, a equipe de administração de sistemas pode ter a necessidade de desativar o acesso à rede de um host se esse host estiver interrompendo os serviços de produção).

Sob nenhuma circunstância um funcionário da empresa está autorizado a se envolver em qualquer atividade ilegal de acordo com as leis locais, estaduais e federais enquanto utiliza recursos de propriedade da empresa.

As atividades a seguir (em geral proibidas) não são exaustivas, mas tentam fornecer exemplos e uma estrutura para atividades que se enquadram na categoria de uso inaceitável.

4.5.1 Atividades inaceitáveis em geral

São exemplos de atividades inaceitáveis:

- Jogar, participar de jogos de azar online ou acessar material ofensivo e impróprio;
- Transmitir e-mail não relacionado ao trabalho para destinatários internos ou externos;
- Conduzir negócios pessoais usando recursos da empresa;
- Transmitir qualquer conteúdo que seja ofensivo ou fraudulento;
- Acessar informações que o funcionário não está autorizado a acessar ou que não necessita para realizar seu o trabalho;

- Acessar ou compartilhar software ou material pirateado;

- Tentar interromper ou hackear outros sistemas (interna ou externamente) ou produzir resultados maliciosos, como danificar sistemas, roubar e remover dados e implantar vírus;

- Vender ou fornecer a terceiros dados pessoais de funcionários, clientes, fornecedores e parceiros de negócio.

4.5.2 Atividades inaceitáveis relacionadas com sistemas e redes

São exemplos de atividades inaceitáveis:

- Violações dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredos comerciais, patentes ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não se limitando a instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não sejam devidamente licenciados para uso pela empresa;

- Cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a digitalização e distribuição de fotografias de revistas, livros ou outras fontes protegidas por direitos autorais, música protegida por direitos autorais e a instalação de qualquer software protegido por direitos autorais para o qual a empresa ou o usuário final não tenha uma licença ativa;

- Acessar dados, servidores ou contas para qualquer finalidade que não seja a condução dos negócios da empresa, mesmo se tiver acesso autorizado;

- A exportação de software, informações técnicas e tecnologias em geral;
- Introdução de programas maliciosos na rede ou servidor (por exemplo, vírus, worms, trojan, bombas de e-mail, etc.).
- Revelar a senha da sua conta a terceiros ou permitir o uso da sua conta por terceiros. Isso inclui a família e outros membros da família quando o trabalho estiver sendo realizado em casa;
- Usar equipamentos de informática de propriedade da empresa para se envolver ativamente na aquisição ou transmissão de material que envolva assédio moral, assédio sexual, violência, ódio, racismo, xenofobia, preconceito, pornografia ou pornografia infantil;
- Usar equipamentos e sistemas da empresa para fazer ofertas fraudulentas de produtos, itens ou serviços;
- Fazer declarações, explícitas ou implícitas, sobre garantia de produtos ou serviços, exceto se for parte das funções normais do trabalho;
- Praticar violações de segurança ou interrupções na comunicação de rede (as violações de segurança incluem, mas não estão limitadas a acessar dados dos quais o funcionário não é o destinatário pretendido ou fazer login em um servidor ou conta que o funcionário não está expressamente autorizado a acessar, a menos que essas funções estejam dentro do escopo das suas funções regulares);
- Realizar varreduras de portas ou varreduras de segurança/vulnerabilidades sem autorização expressa da empresa;

- Executar qualquer forma de monitoramento de rede que intercepte dados não destinados ao host do funcionário, a menos que essa atividade faça parte das funções do funcionário;

- Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta;

- Introduzir honeypots, honeynets ou tecnologia semelhante na rede da empresa;

- Interferir ou negar serviço a qualquer usuário que não seja o host do funcionário (por exemplo, ataque de negação de serviço).

- Usar qualquer programa, script ou comando ou enviar mensagens de qualquer tipo, com a intenção de interferir ou desabilitar a sessão do terminal de um usuário, por qualquer meio, localmente ou via Internet / Intranet;

- Tentar acessar ou obter dados pessoais de funcionários, clientes, fornecedores e parceiros de negócio, exceto se tal atividade fizer parte de suas funções ou tarefas.

4.5.3 Atividades inaceitáveis relacionadas com e-mail e comunicação

Ao utilizar os recursos da empresa para acessar e usar a Internet, os usuários devem sempre ter em mente que, de uma forma ou de outra, representam a empresa.

São exemplos de atividades inaceitáveis:

- Enviar mensagens utilizando contas de e-mail pertencentes à empresa sem que na mesma constem claramente que “os comentários,

mensagens e/ou opiniões não representam necessariamente a opinião da empresa e/ou são endossados pela empresa";

- Enviar mensagens de e-mail não solicitadas, incluindo o envio de "lixo eletrônico" ou outro material publicitário a indivíduos que não solicitaram, especificamente spam por e-mail;

- Qualquer forma de assédio moral ou sexual realizada por e-mail, telefone ou softwares ou aplicativos de mensagens instantâneas;

- Uso não autorizado ou falsificação de informações de cabeçalho de e-mail;

- Solicitação de e-mail para qualquer outro endereço de e-mail, exceto o da conta do autor da postagem, com a intenção de assediar ou coletar informações;

- Criar ou encaminhar "correntes" ou esquemas de "pirâmide" de qualquer natureza;

- Fornecer informações ou listas de funcionários da empresa para terceiros;

- Fornecer a terceiros dados pessoais de funcionários, clientes, fornecedores e parceiros de negócio.

4.5.4 Atividades inaceitáveis relacionadas com blogs e mídias sociais

- A criação e/ou utilização de blogs pessoais e mídias sociais através de sistemas e equipamentos da empresa ou sistemas e equipamentos pessoais do funcionário, também estão sujeitos aos termos e restrições estabelecidos nesta Política. O uso limitado e ocasional dos sistemas e

equipamentos da empresa para a criação e utilização de blogs e mídias sociais é aceitável, desde que feito de maneira profissional e responsável, não viole as políticas da empresa, não seja prejudicial à empresa e não interfira nas obrigações a atividades diárias do funcionário;

- As políticas voltadas à segurança de informações da empresa também se aplicam aos blogs e mídias sociais. Desta forma, ao utilizarem essas plataformas os funcionários estarão proibidos de revelar qualquer informação confidencial ou proprietária da empresa, segredos comerciais, dados pessoais ou qualquer outro material coberto pelas políticas voltadas à segurança de informações da empresa;

- Os funcionários não devem se envolver em nenhum blog ou mídia social que possa prejudicar ou manchar a imagem ou reputação da empresa ou de qualquer um de seus funcionários. Os funcionários também estão proibidos de fazer qualquer comentário discriminatório, depreciativo, difamatório ou de assédio ao utilizarem essas plataformas;

- Os funcionários também não podem fazer declarações pessoais, opiniões ou crenças em nome da empresa ao utilizarem essas plataformas;

- Ao utilizarem blogs ou mídias sociais para expressar suas crenças e opiniões, o funcionário não poderá, explícita ou implicitamente, se apresentar como funcionário ou representante da empresa. Nestes casos o funcionário assumirá todo e qualquer risco associado às suas convicções, crenças e opiniões;

- Publicar dados pessoais de funcionários, clientes, fornecedores e parceiros de negócio;

- Além de seguir todas as leis relativas ao manuseio e divulgação de materiais protegidos por direitos autorais, as marcas registradas, logotipos e qualquer outra propriedade intelectual pertencente à empresa também não poderão ser utilizados nestas plataformas.

5 Responsabilidade

É responsabilidade de cada gestor de departamento, área, setor ou unidade da empresa garantir a aplicação desta norma.

6 Verificação da Conformidade

A equipe de TI, o departamento de RH e os gestores de cada departamento, área, setor ou unidade da empresa verificará a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a, walk-thrus periódicos, logs de auditoria de sistemas e banco de dados, auditorias de TI e feedbacks para o responsável pela política.

Qualquer mudança nesta política deve ser aprovada pelo departamento de TI.

7 Exceções

Não há exceções a esta política. Qualquer exceção à esta norma deverá ser previamente aprovada pela equipe de TI.

8 Violação

Qualquer violação desta norma pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho. A empresa reserva-se o direito de notificar as autoridades responsáveis pela aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade. A empresa não considera que a conduta que viole esta norma esteja dentro do curso e âmbito das atividades de um funcionário, parceiro ou prestador de serviço, ou como consequência direta da execução de suas funções. Consequentemente, na

medida do permitido por lei, a empresa reserva-se o direito de não defender ou pagar quaisquer danos concedidos aos funcionários, parceiros ou prestadores de serviços que resultem da violação desta norma.

9 Aprovação

Responsável	Cargo/Função	Data
LEMUEL VICTOR DIAS	ADVOGADO	18/10/2021
Aprovado por	**Cargo/Função**	**Data**
EDGAR ROBERTO THEODORO	DIRETOR	19/10/2021

10 Histórico de versões

Versão	Descrição	Última Revisão	Próxima Revisão	Revisor/ Aprovador
1.0	Versão inicial	01/03/2021	01/03/2022	