Política de uso aceitável de dispositivos móveis pessoais (BYOD)

Norma #	Vigência	Versão
	01/10/2021	1.0

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

Índice:

1 Visão Geral 1

2 Aplicabilidade 2

3 Norma 2

4 Responsabilidade 6

5 Verificação da conformidade 7

6 Exceções 7

7 Violação 7

8 Aprovação 8

9 Histórico de revisão 8

1 Visão Geral

BYOD ("Bring Your Own Device", em inglês ou "Traga seu Próprio Dispositivo", em português) refere-se à tendência de funcionários usarem dispositivos pessoais para se conectar às redes organizacionais e acessar sistemas relacionados ao trabalho e dados potencialmente sensíveis ou confidenciais. Dispositivos pessoais podem incluir smartphones, computadores pessoais, tablets ou drives USB.

À medida que mais e mais organizações apoiam os funcionários que trabalham em casa, mantendo uma programação flexível ou conectando-se em qualquer lugar durante viagens de trabalho ou viagens, as soluções BYOD se tornaram mais prevalentes. Algumas empresas podem sancionar o BYOD, enquanto outras podem considerá-lo como software ou hardware sem suporte de TI.

Os programas de **BYOD ("Bring Your Own Device", em inglês ou "Traga seu Próprio Dispositivo", em português)** estão se tornando cada vez mais populares, pois oferecem aos funcionários a oportunidade de escolher e comprar seus próprios equipamentos de TI, para uso comercial e pessoal.

Este documento define recomendações e requisitos de uso, ao conectar dispositivos pessoais à rede da MEDICAMENTAL DISTRIBUIDORA LTDA.

A MEDICAMENTAL suporta BYOD, permitindo que funcionários comprem dispositivos de computação móvel pessoal de sua escolha e acessem os sistemas de TI da MEDICAMENTAL. Este documento se aplica, mas não está limitado aos seguintes dispositivos:

- Telefones inteligentes (smartphones);
- Computadores tablet;
- Computadores portáteis (Notebooks);
- Dispositivos de armazenamento portáteis.

Dada a mudança no cenário das tecnologias BYOD, a MEDICAMENTAL deve estar ciente de quaisquer novos dispositivos que possam ser usados para se conectar à rede MEDICAMENTAL. Os dispositivos BYOD representam um risco para os sistemas de tecnologia da informação da MEDICAMENTAL se não forem gerenciados adequadamente e devem ser controlados pelo proprietário de acordo com as recomendações descritas neste documento

Este documento se aplica a todos os usuários, incluindo (mas não se limitando a) funcionários (incluindo eventuais), consultores e contratados, terceiros, funcionários de agências, ex-alunos, associados e honorários, nomeações conjuntas e visitantes da MEDICAMENTAL.

2 Aplicabilidade

Esta norma se aplica:

- À todas as unidade, áreas, setores e departamentos da empresa.

- À 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.

3 Norma

A MEDICAMENTAL se reserva o direito de desconectar qualquer dispositivo que coloque o ambiente MEDICAMENTAL em risco.

O suporte de TI para dispositivos BYOD é fornecido apenas com base nos melhores esforços. Os proprietários de dispositivos são incentivados a seguir os controles detalhados neste documento.

A MEDICAMENTAL monitorará o uso do dispositivo de acordo com as normas estabelecidas de Uso Aceitável, Privacidade e Vigilância no Local de Trabalho.

3.1. Smartphones e Tablets

Lembre-se de que seu smartphone ou tablet é um computador, portanto, devem ser empregadas as melhores práticas para proteger suas informações pessoais, e comerciais.

Certifique-se de que o sistema operacional e os softwares “Apps” instalados estejam atualizados para proteger contra vulnerabilidades conhecidas.

Configure uma senha para obter acesso ao seu dispositivo para proteção contra acesso não autorizado.

Instale um gerenciador de senhas para armazenar seus nomes de usuário, senhas e outras informações confidenciais.

Aproveite os controles de acesso biométrico do dispositivo, se disponíveis.

Defina um tempo limite de inatividade que bloqueará automaticamente o dispositivo quando não estiver em uso. Isso também ajuda a prevenir o acesso não autorizado.

Instale o software de solução de segurança padrão da indústria, com recursos de antivírus, firewall e inteligência contra ameaças.

Execute verificações de vírus regulares.

Obtenha "Apps" apenas de fontes confiáveis para prevenir contra malware que pode ser distribuído por canais não confiáveis.

Não faça "jailbreak" ou "root" (processo que permite aparelhos celulares executar aplicativos não-autorizados pelo fabricante) em seu dispositivo, pois isso remove a proteção do fabricante contra malware.

Faça backups regulares de dados para garantir que suas informações estejam disponíveis, caso seu dispositivo seja perdido, roubado, quebrado ou dados corrompidos.

Apenas armazene informações confidenciais da MEDICAMENTAL em seu dispositivo se for absolutamente necessário (ou seja, necessidades de negócio justificadas). Certifique-se de que as informações confidenciais sejam criptografadas.

Se você armazenar informações confidenciais em seu dispositivo, certifique-se de que sejam removidas com segurança ou transferidas para um local seguro quando não forem mais necessárias.

Se você compartilha seu dispositivo com amigos ou familiares, restrinja o acesso às informações confidenciais da MEDICAMENTAL armazenadas em seu dispositivo.

Registre seu dispositivo em um serviço "Find My Phone" (encontre meu telefone) para localizar e limpar seu dispositivo em caso de perda ou roubo.

Registre os detalhes do seu celular em caso de roubo. Cada celular possui um Identificador Internacional de Equipamento de Estação Móvel (IMEI) exclusivo. A maioria dos telefones permite que você encontre seu IMEI digitando * # 06 #. Saber esse número ajudará seu provedor a impedir que seu telefone seja usado em caso de roubo.

Etiquete seu dispositivo com seu nome e número de telefone, para que ele possa ser devolvido em caso de roubo ou perda, mesmo que a bateria acabe.

No caso de um dispositivo contendo informações da MEDICAMENTAL ser perdido ou roubado, relate o incidente à unidade de suporte de TI local através do telefone (16) 3505-4900 ou envie uma mensagem para ramia@medicamental.com.br.

Ao reciclar seu telefone, certifique-se de excluir todas as informações MEDICAMENTAL existentes e redefina o dispositivo para as configurações de fábrica.

Empregue medidas de segurança física razoáveis ao viajar com o seu dispositivo ou quando estiver na MEDICAMENTAL.

3.2. Notebooks/Laptops

Certifique-se de que todos os patches de segurança do sistema operacional, firmware e aplicativo foram aplicados, para proteger contra vulnerabilidades conhecidas.

Configure seu dispositivo com uma senha forte ou frase de fase.

Instale um gerenciador de senhas ou de segurança segura para armazenar seus nomes de usuário, senhas e outras informações confidenciais.

Aproveite os controles de acesso biométrico do dispositivo, se disponíveis.

Defina um tempo limite de inatividade que bloqueará automaticamente o dispositivo quando não estiver em uso. Isso também ajuda a prevenir o acesso não autorizado.

Instale o software de solução de segurança padrão do fabricante, com recursos de antivírus, firewall e inteligência contra ameaças.

Execute verificações de vírus regulares e resolva problemas.

Obtenha aplicativos apenas de fontes confiáveis, para evitar malware que pode ser distribuído por canais não confiáveis.

Faça backups regulares de dados para garantir que suas informações estejam disponíveis, caso seu dispositivo seja perdido, roubado, quebrado ou dados corrompidos.

Somente armazene informações confidenciais da MEDICAMENTAL em seu dispositivo se for absolutamente necessário. Certifique-se de que as informações confidenciais sejam criptografadas.

Se você armazenar informações confidenciais em seu dispositivo, certifique-se de que sejam removidas com segurança ou transferidas para um local seguro quando não forem mais necessárias.

Se você compartilha seu dispositivo com amigos ou familiares, restrinja o acesso às informações confidenciais da MEDICAMENTAL armazenadas em seu dispositivo.

Etiquete seu dispositivo com seu nome e número de telefone, para que ele possa ser devolvido se for roubado ou perdido, mesmo se a bateria acabar

No caso de um dispositivo contendo informações da MEDICAMENTAL ser perdido ou roubado, relate o incidente à unidade de suporte de TI local ou ao Service Desk no telefone (16) 3505-4900 ou envie um e-mail para ramia@medicamental.com.br.

Ao reciclar seu dispositivo, certifique-se de excluir todas as informações da MEDICAMENTAL residentes.

Empregue medidas de segurança física razoáveis ao viajar com o seu dispositivo ou quando estiver nas dependências da MEDICAMENTAL

3.3. Pendrives e Serviços de Armazenamento em Nuvem

Execute uma varredura antivírus em todas as mídias portáteis (USB) antes de executar os arquivos.

Apenas armazene informações confidenciais da MEDICAMENTAL em seu dispositivo ou na nuvem se for absolutamente necessário, ou seja, necessidade acadêmica, de pesquisa ou de negócios justificada. Certifique-se de que as informações confidenciais sejam criptografadas.

Se você armazenar informações confidenciais em seu dispositivo ou na nuvem, certifique-se de que sejam removidas com segurança ou transferidas para um local seguro quando não forem mais necessárias.

3.4. Wi-Fi e Bluetooth

A MEDICAMENTAL permite que os proprietários de BYOD se conectem à rede sem fio da MEDICAMENTAL para acessar os sistemas da MEDICAMENTAL e a Internet. Os seguintes controles são considerados obrigatórios:

- O acesso deve ser autenticado (e.g., 802. 1x certificado ou nome e senha) antes da conexão na rede da MEDICAMENTAL.
- Os logs de segurança criados pela rede sem fio devem ser gerenciados de acordo com o padrão estabelecidos pelo setor de T.I da MEDICAMENTAL.
- Os indivíduos devem cumprir as regras de uso, conforme descrito na política de uso aceitável de equipamentos de TI da MEDICAMENTAL em todos os momentos.
- Deve-se habilitar o Bluetooth apenas quando necessário para reduzir o risco de atividades maliciosas.
- Deve-se evitar dispositivos que executam versões do Bluetooth anteriores à V4, pois são mais suscetíveis à vulnerabilidade.

4 Responsabilidade

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

5 Verificação da Conformidade

A equipe de TI, verificará a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a auditorias de TI, logs de auditoria de sistemas e banco de dados e feedbacks para o responsável pela política.

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

6 Exceções

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

7 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.

8 Aprovação

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

9 Histórico de versões

Versão	Descrição	Última Revisão	Próxima Revisão	Revisor/ Aprovador
1.0	Versão inicial	15/10/2021	15/10/2022	
