Política de uso e de segurança de dispositivos móveis

Norma #	Vigência	Versão
05	01/03/2021	1.0

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

Índice:

1 Visão geral

Dispositivos móveis são comumente usados para conduzir os negócios da empresa, o que pode torná-los mais suscetíveis a riscos do que desktops ou mesmo laptops. Os desktops são rotineiramente dispositivos fixos e os laptops são mais difíceis de perder do que smartphones ou tablets. Além disso, a mesma engenharia social, phishing e vulnerabilidades do sistema operacional que afetam desktops e laptops são aplicáveis a dispositivos móveis. Com isso em mente, é importante estabelecer e seguir diretrizes específicas e abrangentes para proteger dispositivos móveis contra perda, ataque ou uso indevido.

2 Objetivo

O objetivo desta política é fornecer diretrizes para as necessidades de segurança de dispositivos móveis a fim de proteger as empresas e seus funcionários.

3 Aplicabilidade

Esta norma se aplica:

- À todas as unidades, 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.

4 Norma

4.1. Diretrizes para usuários

Todo uso de dispositivos móveis da empresa deve ser exclusivamente para fins comerciais e profissionais.

Através desses dispositivos devem ser acessadas apenas as informações que são necessárias para realizar o trabalho ou ajudar outros a fazê-lo como parte do escopo válido das funções do funcionário.

Não deve haver o compartilhamento de dispositivos com outros funcionários ou pessoas que não sejam da empresa.

Os dispositivos devem ser protegidos com senhas, PINs ou mecanismos biométricos. Esses mecanismos nunca devem ser contornados ou desativados.

Senhas privadas nunca devem ser compartilhas com quem não está autorizado a tê-las, nem deixadas senhas em um local acessível (como em um post-it).

As senhas devem ser alteradas sempre que se suspeitar que outras pessoas possam ter tido acesso a elas.

As senhas nunca devem ser armazenadas no dispositivo.

Sempre que possível, deve-se salvar todas as senhas de dispositivos móveis compartilhadas em um banco de dados de senhas centralizado e criptografado, como Password Safe ou KeePass. A senha principal desses bancos de dados também deve ser mantida em sigilo e fornecida apenas para indivíduos autorizados.

Os dispositivos móveis devem ser etiquetados com as informações de contato do funcionário para que possam ser devolvidos em caso de perda.

Redes não seguras (com ou sem fio) não devem ser utilizadas.

Se possível, utilizar um MiFi portátil ou Tethering por meio de um dispositivo equipado com acesso à Internet para evitar o uso de redes desconhecidas.

A VPN da empresa deve sempre ser utilizada para se conectar aos recursos da empresa.

O Bluetooth e outros serviços desnecessários deve ser sempre desligado.

Aplicativos não autorizados ou pirateados nunca devem ser instalados nos dispositivos móveis.

Apenas softwares/aplicativos de propriedade da empresa e/ou autorizados pelo departamento de TI devem ser instalados.

Esses aplicativos não devem ter de acesso total a um dispositivo móvel ou aos dados nele contidos.

Todos os dispositivos móveis devem conter e executar software anti-malware. Eles devem ser atualizados regularmente.

Todos os patches de segurança e atualizações do sistema operacional devem ser instalados periodicamente.

Os softwares anti-malware nunca devem ser desabilitados ou contornados e as instalações de patches de segurança e atualizações do sistema operacional nunca devem ser impedidos ou atrasados.

Apenas arquivos de fontes confiáveis devem ser baixados para os dispositivos móveis e somente para fins comerciais.

Todos os sistemas que lidam com esses arquivos devem ter programas anti-malware atualizados que não devem ser desabilitados ou adulterados.

Apenas as permissões apropriadas para aplicativos devem ser permitidos.

Uma verificação de vírus em todos os arquivos executáveis recebidos pela Internet deve sempre ser realizada.

Se um vírus for encontrado (durante uma varredura ou por meio de uma verificação por software anti-malware), o dispositivo deve ser desligado e o departamento de TI deve ser imediatamente informado. Nenhuma outra ação deve ser realizada até receber instruções do departamento de TI.

Como os dispositivos móveis geralmente não têm um cursor para passar o mouse sobre links potencialmente suspeitos para revelar o verdadeiro endereço de um web site (uma maneira comum de detectar tentativas de phishing) deve-se evitar o acesso a esses links em um dispositivo móvel. Um laptop ou desktop deve ser utilizado para analisar o endereço destes web sites.

Material confidencial ou protegido por direitos autorais não deve ser acessado ou visualizado ssem autorização.

Materiais protegidos por direitos autorais não devem ser copiados ou transferidos sem permissão.

As instruções, conselhos e diretrizes sobre riscos de segurança (incluindo engenharia social e riscos de malware) comunicados pelo departamento de TI devem ser seguidos.

A transmissão de informações privadas ou confidenciais por meio de dispositivos móveis devem ser evitadas.

Se for necessário transmitir esses dados, devem ser tomadas medidas destinadas a garantir que as informações sejam entregues à pessoa adequada, que está autorizada a receber essas informações para um uso legítimo.

O compartilhamento e o armazenamento de informações privadas ou confidenciais, devem ser feitos adotando restrições de segurança (por exemplo, via transmissão ou mídia criptografada).

Informações privadas ou confidenciais não devem ser mantidas em mídias não seguras, dispositivos de propriedade do funcionário, dispositivos não seguros, como pen drives ou laptops, ou aplicativos de armazenamento em nuvem de propriedade do funcionário.

Nenhuma cópia de dados deve ser armazenada em qualquer dispositivo móvel. Cópias secundárias devem ser feitas e mantidas em um servidor da empresa e realizadas periodicamente por meios seguros, como conexões VPN.

Nenhum dado pessoal ou dado sensível, deve ser mantido em dispositivos móveis.

Os sistemas da empresa nunca devem ser acessados ou conectados através de quaisquer unidades de mídia removível, unidades USB ou outra mídia de armazenamento de origem desconhecida.

Tentativas de jailbreak ou de root não devem ser realizadas em dispositivos de propriedade da empresa usados para negócios da empresa, pois isso pode levar a riscos de segurança.

Chamadas desconhecidas ou spam devem ser bloqueadas utilizando os recursos de bloqueio de chamadas do dispositivo.

Dispositivos móveis devem sempre ser mantidos sob o controle de funcionários autorizados (não devem ser entregues a ninguém para serem verificadas, despachadas ou transportados).

Cuidados especiais devem ser empregados em aeroportos, estações de trem, terminais de ônibus e outras áreas de tráfego intenso para evitar a perda ou o roubo do dispositivo.

Estações de carregamento USB públicas não devem ser utilizadas em aeroportos ou estações de trem, pois dados podem ser coletados. Deve-se utilizar um carregador USB portátil pessoal.

Se for realmente necessário usar uma estão de carregamento USB pública, deve-se utilizar um dispositivo de proteção como o Juice Jack Defender, que restringe o acesso a dados enquanto carrega um dispositivo.

Os funcionários da empresa devem procurar sempre estar ciente do que está ao seu redor e ficar atento a estranhos que possam tentar ver ou ouvir detalhes comerciais confidenciais sendo compartilhados ou discutidos através de dispositivos móveis.

Dispositivos móveis não devem ser deixados visíveis em veículos desacompanhados, mesmo se estiverem trancados.

Dispositivos móveis não devem ser deixados desprotegidos em quartos de hotel. Deve-se utilizar um cofre para guarda-los ou um cabo de segurança para prendê-los.

O departamento de TI deve ser imediatamente notificado se o dispositivo for perdido ou roubado (especialmente se for um dispositivo autorizado a se conectar aos recursos, sistemas e redes da empresa).

Os funcionários da empresa devem se familiarizar com o processo de uso do Find my iPhone ou Google Find My Device para que possam procurar um dispositivo móvel perdido, caso haja necessidade.

O departamento de TI deve ser notificado imediatamente, caso o funcionário acredite que um dispositivo pessoal ou fornecido pela empresa possa estar infectado por uma ameaça de malware ou de alguma forma comprometido (especialmente se for um dispositivo autorizado a se conectar aos recursos, sistemas e redes da empresa).

O descarte de dispositivo autorizado a se conectar aos recursos, sistemas e redes da empresa deve ser previamente aprovado pelo departamento de TI.

Todos os sistemas ou dispositivos de propriedade da empresa entregues ao funcionário devem ser devolvidos após a rescisão do contrato de trabalho.

Todos os sistemas ou dispositivos de propriedade do funcionário que se conectam aos recursos, sistemas e redes da empresa devem ser enviados ao departamento de TI para inspeção após a rescisão do contrato de trabalho.

Após a rescisão do contrato de trabalho o departamento de TI deve ser informado sobre todas as senhas, dados, informações sigilosas, etc. que devem ser transferidos para os outros funcionários.

O departamento de TI tem o direito de limpar remotamente qualquer dispositivo caso tenha sido perdido ou se após a rescisão do contrato de trabalho o funcionário não o tiver devolvido à empresa.

4.2. Diretrizes para o departamento de TI

Sempre que possível, o departamento de TI deve aplicar políticas de segurança centralizadas aos dispositivos móveis conectados aos recursos, sistemas e rede da empresa.

Se utilizar estratégias de gerenciamento centralizado de dispositivos móveis, deve-se colocar na lista de permissões apenas os aplicativos e configurações apropriados e conceder apenas as permissões adequadas aos aplicativos.

As alterações de senha devem ser aplicadas aos dispositivos móveis no mínimo a cada 60 dias.

O departamento de TI deve oferecer suporte a métodos de conectividade remota segura para dispositivos móveis para acessar os recursos da empresa, por meio de uma conexão VPN criptografada.

O departamento de TI deve certificar que todos os dispositivos móveis executam softwares anti-malware e que estes sejam atualizados regularmente. Garantir que todos os patches de segurança críticos e atualizações do sistema operacional sejam instalados nos dispositivos móveis em uma base periódica. Certificar que os funcionários não possam desligar o software anti-malware nem impedir ou atrasar a instalação de patches de segurança e atualizações do sistema operacional.

O departamento de TI deve sempre reinstalar o sistema operacional e os aplicativos em qualquer dispositivo móvel que tenha sido comprometido ou com suspeita de comprometimento.

Após a rescisão do contrato de trabalho o departamento de TI deve apagar dos dispositivos móveis pessoais (BYOD) do funcionário todos os dados protegidos, sensíveis, confidenciais e de propriedade da empresa.

5 Responsabilidade

É responsabilidade do departamento de TI e 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	