OS DEZ MANDAMENTOS DO BYOD

MaaS360
by Fiberlink

MaaS360® by Fiberlink, an IBM company

Deverás permitir o BYOD

A rápida proliferação dos da entrada de dispositivos móveis no ambiente de trabalho parece uma intervenção divina para muitos dos líderes de TI. É como se uma você ressoando do fundo da montanha ordenasse que todos os funcionários para aos quais você presta suporte adquirissem o maior número possível de dispositivos e os conectassem em massa aos serviços corporativos. O Bring Your Own Device (BYOD) nasceu e os funcionários o seguiram fervorosamente.

Não faz sentido fingir que isso não está acontecendo e dizer "Não permitimos que nossos funcionários façam isso". A verdade que ele eles já estão fazendo isso e continuarão a colocar dispositivos fora de conformidade em sua rede com ou sem a sua permissão. Um estudo do Forrester que envolveu funcionários do setor de informações nos EUA revelou que 37% estão fazendo alguma coisa com tecnologia antes que sejam instituídas permissões ou políticas formais [1] Além disso, uma pesquisa do Gartner com os CIOs determinou que 80% dos funcionários estarão qualificados a usar seus próprios equipamentos com dados do funcionários integrados em 2016. [2]

Isso levanta uma questão inevitável: como você poderá dar suporte aos funcionários que desejam usar seus aplicativos e dispositivos pessoais permitindo que eles sejam produtivos em um ambiente seguro que protege os dados corporativos? Os Dez Mandamentos do BYOD mostram como criar um ambiente móvel pacífico, seguro e produtivo.

OS Dez Mandamentos do BYOD

1. Criarás a política antes de adquirir a tecnologia
2. Procurarás pelos dispositivos do rebanho
3. A inscrição deverá ser simples
4. Deverás configurar os dispositivos para que não necessitem de conexão física
5. Proporcionarás autoatendimento a teus usuários
6. Manterás segredo de informações pessoais sagradas
7. Abrirás os mares entre os dados corporativos e pessoais
8. Monitorarás teu rebanho — Reunirás automaticamente tuas ovelhas
9. Gerenciarás tua utilização dos dados
10. Beberás das fontes do ROI.

[1] Benjamin Gray and Christian Kane, “Fifteen Mobile Policy Best Practices,” Forrester Research, janeiro de 2011.

[2] Ken Dulaney and Paul DeBeasi, “Managing Employee-Owned Technology in the Enterprise,” Gartner Group, outubro de 2011.

MaaS360® by Fiberlink, an IBM company

1. Criarás a política antes de adquirir a tecnologia

Como em qualquer outro projeto de TI, a política precede a tecnologia. Sim, isso acontece até mesmo na nuvem. Para aproveitar efetivamente a tecnologia de MDM (gerenciamento de dispositivos móveis) para os dispositivos de funcionários, você ainda precisa decidir sobre as políticas. Estas políticas afetam mais do que simplesmente a TI. Elas têm implicações para RH, jurídico e segurança — todos os departamentos de empresa que usam os dispositivos moveis em nome da produtividade.

Como todas as linhas de negócios são afetadas pela política de BYOD, ela não pose ser criada em um vácuo de TI. Com as mais diversas necessidades dos usuários, a TI deve garantir que elas estão em todas as partes da criação da política.

Não existe uma política correta de BYOD, mas há algumas questões a serem consideradas:

- **Dispositivos**: Quais dispositivos móveis serão compatíveis? Somente determinados dispositivos ou aqueles que o funcionário quiser?

De acordo com o Forrester, 70% dos smartphones pertencem aos usuários, 12% são opções de uma lista aprovada e 15% são para uso corporativo. Aproximadamente 65% dos tablets pertencem aos usuários, 15% são opções de uma lista e 15% são para uso corporativo. Em outras palavras, na maioria dos casos, os usuários trazem seus próprios dispositivos.

- **Planos de dados:** A organização pagará totalmente pelo plano de dados? Você estipulará um valor mensal ou o funcionário enviará relatórios de despesas?

Quem paga por esses dispositivos? Para smartphones, 70% pagam o preço total, 12% têm desconto, 3% pagam um valor parcial e em 15% dos casos, a empresa cobre o preço total. Com os tablets, 58% compram seu próprio dispositivo, 17% têm um desconto, 7% compartilham os custos e 18% foram comprados e pacos por suas empresas. (Fonte: Forrester, 2011)

- **Conformidade:** Quais regulamentações controlam os dados que sua organização precisa proteger? Por exemplo, a lei americana Health Insurance Portability and Accountability Act (HIPAA) exige criptografia nativa em qualquer dispositivo que contenha dados sujeitos à essa lei.
- **Segurança:** Quais medidas de segurança são necessárias (proteção de senha, dispositivos modificados (jailbroken)/com acessos privilegiados de controle (rooted), aplicativos anti-malware, criptografia, restrições de dispositivo, backup do iCloud)?
- **Aplicativos:** Quais aplicativos são proibidos? Varredura de IP, compartilhamento de dados, Dropbox?
- **Contratos:** Existe algum Contrato de Utilização Aceitável (do inglês Acceptable Usage Agreement, conhecido pela sigla AUA) para dispositivos de funcionários com dados corporativos?
- **Serviços:** Que tipos de recursos os funcionários podem acessar? E-mail? Determinadas redes sem fio ou VPNs? CRM?
- **Privacidade:** Quais dados são coletados dos dispositivos dos funcionários? Quais dados pessoais nunca são coletados?

Nenhuma dúvida está fora dos limites quando ela é proveniente de BYOD. Deve haver diálogo franco e honesto sobre como os dispositivos serão usados e como a TI pode, realisticamente, satisfazer a essas necessidades.

2. Procurarás pelos dispositivos do rebanho

Imagine isso Você começa a usar uma solução MDM supondo que sua empresa suporta aproximadamente 100 dispositivos. Você manteve uma planilha meticulosa dos tipos de dispositivo e usuários, de forma que não deverá acontecer nenhuma surpresa. Mas, quando você olha o relatório pela primeira vez, aparecem logo 200 dispositivos. Esse é um cenário real, não é ficção. Ele ocorre com uma frequência muito maior do que você pode imaginar.

Não viva na negação. O que os olhões não vêem o coração certamente sentirá. Entenda o cenário atual de sua população de dispositivos móveis antes de entalhar sua estratégia nas tábuas de pedra. Para fazer isso, você precisa de uma ferramenta que possa se comunicar em tempo real com seu ambiente de e-mail e detectar todos os dispositivos conectados à sua rede corporativa. Lembre-se de que, uma vez que o ActiveSync seja ativado para uma caixa de entrada, normalmente não existem barreiras para a sincronização de vários dispositivos sem o conhecimento da TI.

Todos os dispositivos móveis precisam ser incorporados em sua iniciativa móvel, sendo que seus proprietários precisarão ser notificados de que as novas políticas de segurança em breve estarão vigentes.

3. A inscrição deverá ser simples

Nada produz não conformidade mais rápido do que a complexidade. Depois de identificar os dispositivos a serem inscritos, seu programa de BYOD deve aproveitar uma tecnologia que ofereça uma maneira simples e fácil para adicionar o dispositivo. O processo deve ser simples, seguro e possibilitar, ao mesmo tempo, a configuração do dispositivo.

Em um cenário perfeito, os usuários devem ser capazes de seguir um link de e-mail ou um texto que leve a um perfil de MDM que esteja sendo criado no dispositivo — incluindo aceitar o sempre importante AUA (Acceptable Use Agreement).

> Encare o BYOD como um casamento que tenha o AUA e como um acordo pré-nupcial que garanta uma união harmoniosa.

As instruções devem ajudar os usuários existentes a se inscrever no programa BYOD. Nós recomendamos que os usuários existentes limpem suas contas de ActiveSync para que seja possível isolar e gerenciar os dados corporativos do dispositivo. Os novos dispositivos devem iniciar om um perfil totalmente zerado.

Da perspectiva de TI, você deseja ter a capacidade para inscrever dispositivos existentes em massa ou para os usuários inscreverem eles mesmos os seus dispositivos. Também é necessário autenticar funcionários com um processo básico de autenticação como a senha única (gerada pelo sistema e utilizável somente uma vez) ou usar diretórios corporativos existentes como o Active Directory/ LDAP. Todos os novos dispositivos que tentem acessar recursos corporativos devem ser colocados em quarentena e notificados pela TI. Isso dá à TI a flexibilidade para bloquear ou iniciar um fluxo de trabalho de inscrição apropriado (se aprovado), garantindo a conformidade com as políticas corporativas.

MaaS360® by Fiberlink, an IBM company

4. Deverás configurar os dispositivos para que não necessitem de conexão física

Se existe uma coisa que sua política de BYOD e a solução de MDM não devem fazer é levar mais usuários ao serviço de atendimento ao cliente. Todos os dispositivos devem ser configurados para não necessitar de conexão física a fim de maximizar a eficiência para a TI e usuário comerciais da mesma maneira.

Depois que os usuários aceitarem o AUA, sua plataforma deverá oferecer todos os perfis, credenciais e configurações que o funcionário precisa acessar, inclusive:

- E-mail, contatos e calendário
- VPN
- Documentos corporativos e conteúdo
- Aplicativos internos e públicos

Nesse ponto, você também criará políticas para restringir o acesso a determinados aplicativos e gerar alertas quando um usuário exceder seu limite de utilização de dados ou o limite do valor pago por mês.

5. Proporcionarás autoatendimento a teus usuários

E darás graças por ter feito isso. Os usuários querem ver seu dispositivo funcionando e você deseja otimizar o tempo do serviço de atendimento ao cliente. Uma plataforma de autoatendimento robusta permite que os usuários executem diretamente:

- Redefinição de PIN e senha no caso de o funcionário esquecer os atuais
- Geolocalização de um dispositivo perdido a partir de um portal da Web, usando integração de mapeamento
- Limpeza remota de um dispositivo, removendo todos os dados confidenciais da empresa

Segurança, proteção dos dados corporativos e conformidade são responsabilidades compartilhadas Talvez seja um comprimido difícil de os funcionários engolirem, mas não há possibilidade de reduzir os riscos em a cooperação deles. Um portal de autoatendimento pode ajudar os funcionários a entender as razões pelas quais eles podem estar fora de conformidade.

MaaS360® by Fiberlink, an IBM company

6. Manterás segredo de informações pessoais sagradas

É claro que a política de BYOD não trata simplesmente de proteger dados corporativos. Um programa de BYOD bem formulado mantém os dados dos funcionários intocados e protegidos. É possível usar informações pessoais identificáveis (PII) para identificar, contatar ou localizar uma pessoa. Algumas leis de privacidade impedem até mesmo que as empresas visualizem estes dados. Transmita a política de privacidade as funcionários e deixe claro que os dados não poderão ser coletados de seus dispositivos móveis. Por exemplo, uma solução de MDM deve ser capaz de analisar quais informações podem ser acessada e quais não podem, como:

- E-mail, contatos e calendário pessoais
- Dados de aplicativos e mensagens de texto
- Histórico de chamadas e correios de voz

Por outro lado, permita que os usuários saibam o que você vai coletar, como isso será usado e porque isso os beneficia.

Uma solução avançada de MDM pode transformar a política de privacidade em uma configuração de privacidade para ocultar as informações de localização e de software em um dispositivo. Isso ajuda as empresas a atender às regulamentações de PII e oferece mais conforto para os funcionários evitando a visualização das informações pessoais em smartphones e tablets. Por exemplo:

- Desabilitar o relatório de inventário de aplicativos para impedir os administradores de ver os aplicativos pessoais
- Desativar os serviços de localização para evitar o acesso a indicadores de localização, como endereço físico, coordenadas geográficas, endereço IP e WiFi SSID

Transparência e clareza são pontos de atenção importantes. Há muito menos resistência às políticas de BYOD quando todos conhecem as regras.

7. Abrirás os mares entre os dados corporativos e pessoais

Para que o BYOD seja um acordo com o qual a TI e os usuários finais possam conviver, as informações pessoais como fotos da festa de aniversário ou aquele ótimo romance americano devem ser isoladas de seus aplicativos de produtividade.

Colocando-se de maneira simples, os aplicativos, documentos e outros materiais corporativos devem ser protegidos pela TI se o funcionário decidir deixar a organização, mas os e-mails, aplicativos e fotos pessoais devem permanecer intocados pela TI corporativa.

Não só os usuários apreciam a liberdade dessa abordagem, mas também a TI, cuja fica ficará infinitamente mais fácil como resultado disso. Com esta abordagem, a TI pode limpar dados corporativos seletivamente quando um funcionário deixar a empresa. Dependendo das circunstâncias, se um funcionário perder o dispositivo, o dispositivo inteiro poderá ser limpo. Mas somente uma verdadeira solução de MDM pode oferecer esta opção.

Aproximadamente 86% das limpezas de dispositivo são seletivas, sendo que somente os dados corporativos são limpos.

MaaS360® by Fiberlink, an IBM company

8. Monitorarás teu rebanho — Reunirás automaticamente tuas ovelhas

Depois que o dispositivo estiver inscrito, tudo se resumirá a contexto. Os dispositivos devem ser monitorados continuamente quanto a determinado cenários e as políticas automatizadas devem estar implementadas. O usuário está tentando desativar o gerenciamento? O dispositivo está em conformidade com a política de segurança? Você precisa fazer ajustes com base nos dados que está vendo? Daqui em diante, você começará a entender todas as políticas e regras adicionais a serem criadas. Seguem aqui alguns problemas comuns:

- **Chegar ao "Root" do Jailbreaking:** Para obter gratuitamente aplicativos que deveriam ser pagos, os funcionários algumas vezes modificam ("jailbreak") ou usam programas que proporcionam acesso de controle privilegiado ("root") em um telefone, abrindo a porta para malwares que podem roubar informações. Se um dispositivo é modificado, a solução MDM deve ser capaz de tomar a ação correta, como limpar imediata e seletivamente os dados corporativos do dispositivo.
- **Poupe a limpeza, envie um SMS:** Se os desperdiçadores de tempo como o Angry Birds esbarrarem nas políticas corporativas mas não se configurarem como uma violação, uma limpeza imediata seria um desastre. Uma solução MDM pode impor políticas baseadas em violações. O MDM pode enviar uma mensagem para o usuário oferecendo tempo para que ele remova o aplicativo antes que a TI acione a limpeza.
- **Novos sistemas operacionais disponíveis:** Para o BYOD permanecer eficaz, os usuários precisam de uma maneira simples de ser alertados quando um novo sistema operacional está pronto para instalação. Com a solução de MDM correta, as atualizações de SO se tornam uma função de autoatendimento. Restringir as versões de SO antigas garante a conformidade e maximiza a operabilidade do dispositivo.

9. Gerenciarás tua utilização dos dados

A política BYOD coloca a TI claramente fora do negócio de comunicações, mas a maioria das empresas ainda precisa ajudar os funcionários a gerenciar seu uso de dados a fim de evitar encargos excessivos.

Se você paga pelo plano de dados, talvez você queira rastrear estes dados. Se você não está pagando, talvez queira ajudar os usuários a rastrear suas utilizações de dados atuais. Você deve ser capaz de rastrear os dados na rede e em roaming em dispositivos que geram alertas caso o usuário ultrapasse o limite de utilização dos dados.

Você pode definir os limites em megabits na rede e personalizar o dia da fatura para criar notificações com base no percentual utilizado. Também recomendamos educar os usuários em relação aso benefícios de usar o WiFi quando estiver disponível. A configuração automática de WiFi ajuda a garantir que os dispositivos se conectem automaticamente ao WiFi enquanto estiver nas dependências da empresa.

Se o plano com pagamento mensal cobrir US$ 50 ou 200 Mb de utilização de dados por mês, os funcionários vão gostar de receber um alerta caso estejam prestes a pagar um excesso de limite.

MaaS360® by Fiberlink, an IBM company

10. Beberás das fontes do ROI.

Enquanto o BYOD passa a responsabilidade pela compra de dispositivo para os funcionários, vale observar o quadro completo e os custos de longo prazo para sua organização.

Quando estiver redigindo a política, considere o quanto esta política afetará o ROI. Isso inclui as abordagens de comparação, como mostrado na tabela a seguir.

Modelo de propriedade corporativa	**BYOD**
Quanto você gastaria em cada dispositivo	O custo de um plano de dados parcialmente subsidiado
O custo de um plano de dados totalmente subsidiado	O custo eliminado da compra do dispositivo
O custo dos dispositivos de reciclagem todos os anos	O custo de uma plataforma de gerenciamento móvel
Planos de garantia	
Tempo e mão de obra de TI no gerenciamento do programa	

Um tamanho nunca serve em todas as pessoas, mas uma política de BYOD cuidadosamente formulada fornece a você a orientação que você precisa para gerenciar dispositivos móveis com eficiência e eficácia.

É claro que os aumentos de produtividade são vistos com frequência quando os funcionários são móveis e então conectados o tempo todo. BYOD é uma ótima maneira de trazer esse avanço na produtividade para os novos usuários que podem não estar qualificados para dispositivos corporativos em um primeiro momento.

BYOD: A segurança da liberdade

O BYOD é uma prática recomendada emergente para possibilitar as funcionários a liberdade de trabalhar em seus próprios dispositivos enquanto aliviam a TM de cargas financeiras e gerenciais significativas, mas o BYOD nunca será fornecidos nos locais de gerenciamento simplificado e com redução de custos em uma política bem redigida e uma plataforma de gerenciamento robusta.

Se você está convencido de que o BYOD é a medida correta para seus negócios, clique aqui para começar a usar o MaaS360 por trinta dias gratuitamente. Como o MaaS360 é baseado na nuvem, seu ambiente de teste imediatamente se transforma em ambiente de produção com nenhuma perda de dados.

Se você ainda está nos primeiros estágios de sua estratégia móvel, o MaaS360 oferece uma boa quantidade de recursos educacionais, incluindo o seguinte:

www.maas360.com
http://www.maas360.com/products/mobile-device-management/
MaaSters Center

Para obter mais informações

Para obter mais informações sobre nossa tecnologia e nossos serviços, visite www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Telefone 215-664-1600 | Fax 215-664-1601 | sales@fiberlink.com