IBM Security
Livre blanc « Thought Leadership » (Un leadership des idées)

Les 10 règles du BYOD

Découvrez comment protéger les données d'entreprise lorsque les employés utilisent leurs appareils personnels au travail

IBM

Devez-vous autoriser le BYOD ?

La prolifération rapide des dispositifs mobiles dans l'entreprise s'apparente à un miracle divin pour de nombreux responsables informatiques. Les appareils mobiles et leurs applications ont transformé nos modes de vie, notre façon de communiquer, de voyager, d'acheter, de travailler et bien plus encore. Cette transformation mobile a été tellement brutale, tellement révolutionnaire, qu'il est désormais difficile d'envisager la vie sans ces appareils. Le BYOD (Bring Your Own Device : pratique consistant à utiliser son dispositif de communication personnel au travail) est né, et les employés l'ont très rapidement adopté.

Il sera vain d'ignorer ce phénomène ou de dire « nous l'interdisons à nos employés ». Dans la réalité quotidienne, les employés font du BYOD parfois même sans le savoir et ils continueront à introduire des dispositifs non conformes sur votre réseau, que cela vous plaise ou non. D'ici 2016, la plupart des employés seront autorisés à utiliser leurs propres smartphones et tablettes au travail.

Cette évolution soulève une question évidente : comment allez-vous vous adapter au désir des employés d'utiliser leurs propres appareils et applications tout en leur permettant d'être productifs dans un environnement qui protège les données d'entreprise ? *Les 10 règles du BYOD* vous indiquent comment créer un environnement mobile serein, protégé et productif.

Les 10 règles du BYOD

1. Définissez votre politique avant d'acquérir la technologie
2. Identifiez les dispositifs qui accèdent aux ressources de l'entreprise
3. La connexion doit être simple
4. Configurez vos appareils dans la foulée
5. Aidez vos utilisateurs à se servir
6. Préservez la confidentialité des données personnelles
7. Séparez les données de l'entreprise des données personnelles
8. Gérez l'utilisation des données
9. Surveillez les dispositifs en continu pour vérifier leur conformité
10. Profitez du retour sur investissement engendré par le BOYD

1. Définissez votre politique avant d'acquérir la technologie

Comme pour tout autre projet informatique : d'abord la définition des politiques, puis l'achat des technologies... oui, même dans le cloud. Si vous voulez être sûr que votre technologie MDM (Mobile Device Management - Gestion des appareils mobiles) est utilisée efficacement sur les appareils des employés, vous devez en passer par la définition de politiques. Ces politiques ne concernent pas uniquement le service informatique : elle touchent les RH, le service juridique, la sécurité et tous les composants de l'entreprise qui utilisent les appareils mobiles au nom de la productivité.

Etant donné que tous les services sont concernés par la politique BYOD, il est impossible de s'isoler dans un monde technologico-informatique pour la définir. En effet, le service informatique doit s'assurer que les différents besoins des utilisateurs sont intégrés à la définition de cette politique.

Il n'existe pas de politique BYOD modèle mais il est tout de même nécessaire de répondre à certaines questions :

- **Dispositifs :** Quels seront les appareils mobiles supportés ? Seulement certains ou tous ceux suggérés par les employés ?
- **Plans de données mobiles :** L'entreprise paiera-t-elle pour les plans de données mobiles ? Sous forme de rémunération ou basé sur des notes de frais ?
- **Conformité :** Quelles sont les réglementations régissant les données que votre entreprise doit protéger ? Par exemple, la loi HIPAA (Health Insurance Portability and Accountability Act) exige l'utilisation du chiffrement sur l'ensemble des appareils qui comportent des données concernées par ses dispositions.
- **Sécurité :** Quelles sont les mesures de sécurité à envisager (protection par mot de passe, appareils débridés/rootés, applis contre les logiciels malveillants, chiffrement, restrictions des appareils, sauvegarde iCloud) ?
- **Applications :** Quelles sont les applis interdites ? Analyse IP, partage de données, Dropbox ?
- **Accords :** Est-il possible d'établir un accord d'utilisation acceptable des données d'entreprise avec les utilisateurs ?
- **Services :** Quels types de ressources les employés peuvent-ils ouvrir ? Certains réseaux sans fil ou VPN ? Le CRM ?
- **Confidentialité :** Quelles sont les données collectées à partir des appareils des employés ? Quelles sont les données personnelles à ne jamais collecter ?

Aucune question n'est absurde lorsqu'il s'agit de BYOD. Le dialogue doit être franc et honnête sur l'utilisation des appareils et sur les capacités du service informatique à répondre aux besoins.

2. Identifiez les appareils qui accèdent aux ressources de l'entreprise

Imaginez ce qui suit : Vous commencez à utiliser une solution MDM en supposant que votre entreprise compte environ 100 appareils. Vous tenez méticuleusement une feuille de calcul qui recense les types d'appareils et leurs utilisateurs. Aucune mauvaise surprise n'est donc possible. Cependant, dès le premier rapport, ce sont 200 appareils qui s'affichent. Ce scénario n'est pas fictif, il est bien réel. Il se reproduit bien plus souvent que vous ne pouvez l'imaginer.

Ne vivez pas dans le déni. Dans l'idée que « ce que vous ne savez pas ne vous touche pas ». Etudiez votre environnement mobile actuel avant d'élaborer une stratégie immuable. Pour ce faire, vous devrez vous appuyer sur un outil capable de communiquer en temps réel avec votre environnement de messagerie et de détecter tous les appareils connectés à votre réseau d'entreprise. N'oubliez pas que si ActiveSync est activé sur une boîte de messagerie, il n'y a généralement aucun problème pour synchroniser plusieurs appareils sans que le service informatique le sache.

Votre projet de mobilité doit englober tous les appareils mobiles. De même, les propriétaires de ces appareils doivent être avertis de l'entrée en vigueur de nouvelles politiques de sécurité.

3. La connexion doit être simple

La complexité favorise la non-conformité. Une fois que les appareils ont été identifiés, votre programme BYOD doit intégrer une technologie simple et rapide d'enregistrement des utilisateurs. Ce processus doit être ergonomique et protégé, et capable de configurer l'appareil dans la foulée.

Dans le meilleur des mondes, les utilisateurs devraient pouvoir cliquer sur un lien reçu par courrier électronique qui créerait un profil MDM sur leur appareil et permettrait d'accepter les incontournables accords d'utilisation.

Envisagez le BYOD comme un mariage et les accords d'utilisation comme un contrat prénuptial qui garantit une union heureuse.

Des instructions doivent aider les utilisateurs à s'enregistrer dans le programme BYOD. Il est recommandé de demander aux utilisateurs existants de supprimer leurs comptes ActiveSync pour vous permettre d'isoler et de gérer les données d'entreprise sur l'appareil. Les appareils neufs doivent commencer avec un profil vierge.

Du point de vue du service informatique, vous voulez soit enregistrer les appareils existants en masse, soit demander aux utilisateurs qu'ils les enregistrent eux-mêmes. Vous devez également être en mesure d'authentifier les employés à l'aide d'un processus d'authentification de base, tel qu'un mot de passe à usage unique, ou d'utiliser les répertoires existants tels qu'Active Directory/LDAP. Tous les appareils neufs tentant d'accéder à des ressources de l'entreprise doivent être placés en quarantaine et le service informatique doit en être averti. Ainsi, le service informatique pourra choisir de bloquer l'appareil ou, s'il l'autorise, de lancer un workflow d'enregistrement en bonne et due forme afin de garantir la conformité aux politiques de l'entreprise.

4. Configurez vos appareils dans la foulée

S'il est bien un effet que la politique BYOD et la solution MDM ne doivent pas produire, c'est orienter davantage d'utilisateurs vers le service d'assistance. Vos dispositifs doivent être configurés par connexion sans fil pour optimiser l'efficacité de l'opération pour le service informatique et pour les employés.

Lorsque les utilisateurs ont accepté les accords d'utilisation, votre plateforme doit leur procurer les profils, les identifiants et les paramètres dont ils ont besoin, et notamment :

- La messagerie électronique, les contacts et le calendrier
- Le VPN et le Wi-Fi
- Les documents et les contenus d'entreprise
- Les applis internes et publiques

Ensuite, vous créerez également des politiques pour restreindre l'accès à certaines applis et générer des avertissements si l'utilisateur consomme plus de données que prévu ou dépasse sa limite mensuelle.

5. Aidez vos utilisateurs à se servir

Et vous en serez récompensé. Les utilisateurs veulent un appareil qui fonctionne et vous voulez éviter de faire perdre du temps au service d'assistance. Une plateforme libre-service bien conçue permet aux utilisateurs de réaliser les actions suivantes :

- Réinitialiser un mot de passe en cas d'oubli
- Géolocaliser un appareil perdu à partir d'un portail internet, en utilisant un outil cartographique
- Effacer à distance le contenu d'un appareil pour supprimer les données d'entreprise sensibles

La sécurité, la protection des données de l'entreprise et la conformité sont des responsabilités partagées. Cela peut être difficile à accepter pour les employés, mais il est impossible d'atténuer les risques sans leur coopération. L'utilisation d'un portail libre-service aidera les employés à comprendre pourquoi ils risquent de se trouver en non-conformité.

6. Préservez la confidentialité des données personnelles

Evidemment, la politique BYOD ne concerne pas uniquement la protection des données de l'entreprise. Un programme BYOD bien conçu permet de conserver les données personnelles des employés hors d'atteinte de tous, y compris des membres du service informatique. Les informations d'identification personnelle peuvent également servir à identifier, à contacter ou à localiser une personne. Certaines lois sur la vie privée interdisent même aux entreprises d'afficher ces données. Transférez la politique de confidentialité aux employés et précisez clairement la nature des données que vous ne pourrez pas collecter sur leurs dispositifs mobiles. Ainsi, une solution MDM doit pouvoir faire le tri entre les informations qu'elle peut collecter et celles qui lui sont interdites, par exemple :

- Les courriers électroniques, les contacts et le calendrier personnels
- Les données des applis et les SMS
- Le journal des appels et la messagerie vocale

En revanche, expliquez aux utilisateurs tous les éléments que vous collectez, l'utilisation que vous en ferez et l'intérêt que cela représente pour eux.

Une solution MDM avancée est capable de transformer une politique de confidentialité en paramètre de confidentialité afin de masquer les données logicielles et de géolocalisation d'un appareil. Cela permet aux entreprises de mieux se conformer aux réglementations sur les informations d'identification personnelle. De même, les employés en tirent un certain confort puisque les données personnelles contenues dans leurs smartphones et tablettes ne peuvent pas être visualisées. Ils peuvent, par exemple :

- Désactiver l'inventaire des applis pour éviter que les administrateurs puissent voir les applis personnelles.
- Désactiver les services de géolocalisation pour prévenir l'accès aux informations de ce type, par exemple, l'adresse physique, les coordonnées GPS, l'adresse IP et le SID Wi-Fi.
- Transparence et clarté sont deux mots d'ordre importants. La résistance aux politiques BYOD est nettement moins forte lorsque chaque utilisateur connaît les règles.

7. Séparez les données de l'entreprise des données personnelles

Pour que le BYOD représente un accord viable pour le service informatique et pour les utilisateurs, les informations personnelles telles que les photos de la dernière fête d'anniversaire ou les détails du roman américain du siècle doivent être isolées des applis dédiées à la productivité.

En bref, les applis, les documents et les autres ressources de l'entreprise doivent être protégés par le service informatique si l'employé décide de quitter la société. Par contre, la messagerie, les applis et les photos personnelles doivent demeurer hors de portée du service informatique.

Non seulement la liberté conférée par cette approche sera appréciée par les utilisateurs, mais elle facilitera considérablement la vie du service informatique. Grâce à cette approche, le service informatique pourra effectuer une suppression sélective des données lorsque l'employé quittera l'entreprise. De même, selon les circonstances, il sera possible d'effacer tous le contenu de l'appareil s'il venait à être perdu. Une véritable solution MDM vous laisse le choix.

Selon les estimations, 86 % des effacements d'appareils sont sélectifs et seules les données d'entreprise sont supprimées.

8. Gérer l'utilisation des données

En règle générale, une politique BYOD tient largement le service informatique à l'écart des activités de communication. Toutefois, de nombreuses entreprises doivent encore aider leurs employés à gérer l'utilisation des données afin d'éviter les surcharges.

Si vous payez un plan de données, un suivi des données peut vous être utile. Dans le cas contraire, vous pouvez néanmoins aider les utilisateurs à suivre leur consommation de données. Vous devez être en mesure de suivre la consommation de données des appareils, aussi bien sur le réseau qu'en itinérance, et de générer des alertes si un utilisateur dépasse un certain seuil.

Vous pouvez définir des limites en mégaoctets pour le réseau et l'itinérance, et personnaliser les rapports de facturation afin de créer des notifications basées sur le pourcentage utilisé. Il est recommandé d'expliquer aux utilisateurs les avantages d'utiliser une liaison Wi-Fi lorsqu'ils en ont la possibilité. Une configuration Wi-Fi automatique permet de s'assurer que les appareils se connectent au Wi-Fi dès qu'ils entrent dans le périmètre de l'entreprise.

Si le forfait attribué couvre uniquement 50 $ ou 200 Mo de données par mois, les employés apprécieront de recevoir un avertissement indiquant qu'ils sont responsables de tout dépassement.

9. Surveillez les appareils en continu pour vérifier leur conformité

Une fois l'appareil enregistré, tout dépend du contexte. Dans certains cas, les appareils doivent être surveillés en continu et des politiques automatisées doivent être mises en place. L'utilisateur essaie-t-il de désactiver la gestion ? L'appareil est-il conforme à la politique de sécurité ? Avez-vous besoin d'apporter des ajustements en fonction des données que vous consultez ? Lorsque vous avez les réponses à ces questions, vous pourrez définir les politiques ou règles complémentaires à créer. Voici quelques problèmes courants :

- **Remonter à la source du débridage :** Pour obtenir gratuitement des applis normalement payantes, certains employés « débrident » ou « rootent » leur téléphone, ce qui ouvre la porte à des logiciels malveillants susceptibles de voler des données. Si un appareil est débridé, la solution MDM doit prendre les mesures nécessaires telles que l'effacement sélectif et immédiat des données de l'entreprise.
- **Epargnez-vous un effacement ; envoyez un SMS :** Si des applis inutilement chronophages telles qu'Angry Birds vont à l'encontre de la politique d'entreprise, mais ne représentent pas de danger, l'effacement automatique est une mesure excessive. Une solution MDM peut faire appliquer des politiques en s'adaptant au niveau de danger. La MDM peut envoyer un message à l'utilisateur pour lui laisser le temps de supprimer l'appli avant que le service informatique n'appuie sur le bouton « Effacer ».
- **Nouveau système d'exploitation disponible.** Pour que le BYOD conserve son efficacité, les utilisateurs doivent être avertis lorsqu'un nouveau système d'exploitation est prêt à être installé. Avec une solution MDM appropriée, les mises à≈niveau du système d'exploitation se transforment en fonction libre-service. Limiter la présence de versions obsolètes permet de garantir la conformité tout en optimisant le fonctionnement de l'appareil.

10. Profitez du retour sur investissement engendré par le BOYD

Même si le BYOD transfère la responsabilité d'achat des appareils sur les employés, il est important d'examiner la situation générale et d'étudier les coûts à long terme pour votre entreprise.

Lorsque vous définissez votre politique, tenez compte de son impact sur le retour sur investissement. Ceci inclut la comparaison des approches, comme indiqué ci-dessous :

Modèle avec dispositifs appartenant à l'entreprise

- Combien vous coûterait chaque dispositif ?
- Coût d'un plan de données entièrement subventionné
- Coût du recyclage des appareils après quelques années
- Plans de garantie
- Temps et main d'œuvre consacrés par le service informatique dans la gestion du programme

BYOD

- Coût d'un plan de données partiellement subventionné
- Suppression du coût de l'achat des appareils
- Coût de la plateforme de gestion de la mobilité

Il n'existe pas de solution universelle, mais une politique BYOD minutieusement élaborée peut vous apporter tous les atouts nécessaires pour gérer efficacement les appareils mobiles.

Bien sûr, des améliorations de la productivité sont souvent constatées lorsque les employés sont mobiles et connectés en permanence. Le BYOD est une excellente solution pour étendre ces améliorations de productivité à de nouveaux utilisateurs qui n'ont pas le droit d'utiliser des appareils de l'entreprise.

BYOD : La sécurité de la liberté

Le BYOD est une meilleure pratique émergente qui donne aux employés la liberté de travailler avec leurs propres appareils tout en allégeant les budgets et les contraintes qui pèsent sur le service informatique. Cependant, s'il n'est pas encadré par une politique bien formulée et une plateforme d'administration solide, le BYOD ne peut pas tenir ses promesses de rationaliser la gestion et de réduire les coûts.

Si vous en êtes encore aux prémices de votre stratégie mobile, IBM® MaaS360® vous propose un large éventail de ressources éducatives.

Si vous décidez que le BYOD convient à votre entreprise, cliquez ici pour tester gratuitement MaaS360 pendant 30 jours. MaaS3360 étant basé sur le cloud, votre environnement de test peut devenir automatiquement un environnement de production sans entraîner de perte de données.

A propos d'IBM MaaS360

IBM MaaS360 est une plateforme de gestion de la mobilité d'entreprise qui soutient la productivité et assure la protection des données en fonction des habitudes de travail des utilisateurs. Des milliers d'entreprises font confiance au MaaS360 comme fondation de leurs initiatives mobiles. MaaS360 offre une gestion intégrale, avec de puissants contrôles de sécurité pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter tous les déploiements mobiles. Pour plus d'informations sur IBM MaaS360 et pour commencer un essai gratuit de 30 jours, rendez-vous sur www.ibm.com/maas360

A propos d'IBM Security

La plateforme de sécurité IBM fournit les données de sécurité nécessaires pour aider les entreprises à gérer leurs utilisateurs, leurs données, leurs applis et leur infrastructure de manière globale. IBM propose des solutions de gestion des identités et des accès, de gestion des données et des événements relatifs à la sécurité, la sécurité des bases de données, le développement d'applis, la gestion des risques, la gestion des terminaux, la protection de dernière génération contre les intrusions, etc. IBM possède l'un des plus grands services du monde en matière de recherche, de développement et de mise en œuvre de services de sécurité. Pour en savoir plus, visitez le site : www.ibm.com/security

© Copyright IBM Corporation 2016

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux Etats-Unis
Mars 2016

IBM, le logo IBM, ibm.com et X-Force sont des marques d'International Business Machines Corp. déposées dans de nombreuses juridictions à travers le monde. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® et appareils, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, MaaS360® Secure Mobile Mail, MaaS360® Mobile Document Sync, MaaS360® Mobile Document Editor et MaaS360® Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360® et We do IT in the Cloud.™ sont des marques ou des marques déposées de Fiberlink Communications Corporation, une société IBM. D'autres noms de produits et services peuvent être des marques commerciales d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur le Web à la section « Copyright and trademark information » sur **ibm.com**/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch et iOS sont des marques commerciales ou déposées d'Apple Inc aux Etats-Unis et dans d'autres pays.

Les informations contenues dans ce document sont correctes à la date de leur publication initiale et peuvent être modifiées par IBM à tout moment. Toutes les offres ne sont pas disponibles dans tous les pays où IBM opère.

Les chiffres relatifs aux performances et les exemples de clients cités sont présentés à des fins d'illustration uniquement. Les résultats de performances réels peuvent varier selon les configurations spécifiques et les conditions de fonctionnement. Il incombe à l'utilisateur d'évaluer et de vérifier le fonctionnement de tout autre produit ou programme avec les produits et programmes IBM.

LES INFORMATIONS CONTENUES DANS CE DOCUMENT SONT LIVREES « EN L'ETAT » SANS AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, NOTAMMENT SANS AUCUNE GARANTIE OU CONDITION DE QUALITE MARCHANDE OU D'APTITUDE A UN EMPLOI SPECIFIQUE ET SANS AUCUNE GARANTIE DE NON-CONTREFACON. Les produits IBM sont garantis conformément aux conditions de leur contrat de vente.

Le client est tenu de s'assurer du respect des lois et réglementations en vigueur. IBM ne fournit pas d'avis en matière juridique ; par ailleurs IBM ne fournit aucune garantie quant à la conformité du client aux lois de ses produits et services.

Toutes les déclarations relatives aux orientations futures d'IBM sont sujettes à modification sans préavis. Elles n'expriment que les intentions et les objectifs d'IBM.

Déclaration de bonnes pratiques en matière de sécurité : La sécurité des systèmes informatiques implique la protection des systèmes et des informations en prévenant, détectant et réagissant aux accès non autorisés, qu'ils proviennent de l'entreprise ou de l'extérieur. Les accès non autorisés peuvent entraîner l'altération, la destruction ou l'utilisation inappropriées des informations et ainsi causer des dommages ou un détournement de vos systèmes, par exemple pour attaquer des tiers. Aucun système ou produit informatique ne doit être considéré comme entièrement sécurisé. Aucun produit ni aucune mesure de sécurité ne peut être totalement efficace contre les accès non autorisés. Les systèmes et produits IBM s'inscrivent dans une approche de sécurité complète qui implique des procédures opérationnelles supplémentaires et peuvent demander aux autres systèmes, produits ou services d'être plus efficaces. IBM ne garantit pas que ses systèmes et ses produits sont invulnérables face aux comportements malveillants ou illégaux provenant de tiers.

Pensez à recycler

WGW03112-FRFR-01