# Bonnes pratiques pour une gestion simple et sécurisée des appareils

Une productivité mobile pour votre entreprise.
La liberté de choix pour vos employés.
Une sécurité et un contrôle complets pour votre IT.

La liberté de choix de l'utilisateur est devenue le fondement essentiel des stratégies informatiques modernes. En permettant aux utilisateurs de choisir eux-mêmes les appareils les plus adaptés à leurs besoins, les entreprises améliorent la productivité, la flexibilité d'emploi et la satisfaction de leurs collaborateurs. Avec la bonne stratégie, votre IT peut s'assurer de la mise en place des politiques et technologies appropriées, permettant de protéger les données d'entreprise tout en réduisant les coûts et en garantissant une formidable expérience utilisateur.

Votre stratégie doit permettre à votre organisation :

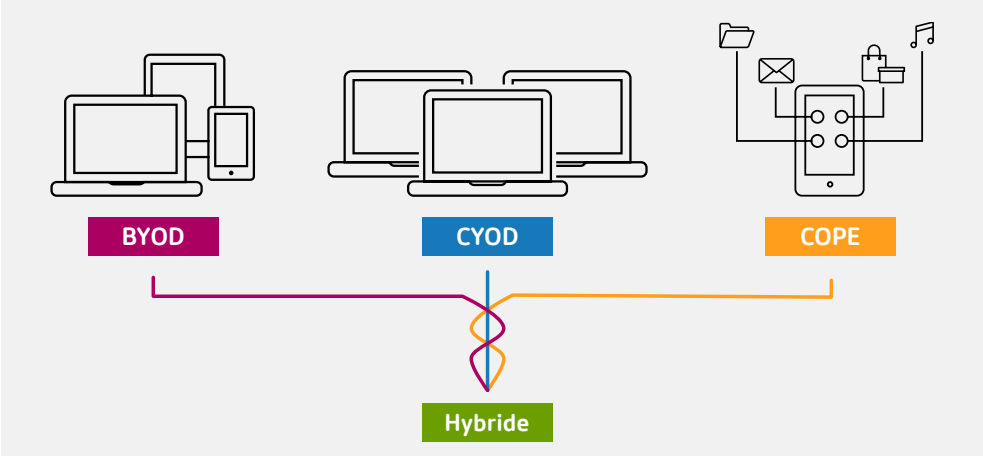
- **De donner de l'autonomie à ses utilisateurs** en les laissant choisir leur propre appareil pour améliorer la productivité, la collaboration et la mobilité.
- **De protéger les informations sensibles** contre la perte et le vol tout en respectant les normes de confidentialité, de conformité et de gestion des risques.
- **De réduire les coûts et de simplifier la gestion** grâce au provisioning en libre-service et à l'automatisation de l'administration et de la supervision.
- **De simplifier l'informatique** grâce à une unique solution complète pour sécuriser et administrer les données, les applications et les appareils.

Voici 8 bonnes pratiques pour concevoir une stratégie associant la simplicité pour les collaborateurs à un contrôle, une sécurité et une administration efficaces pour l'équipe IT :

### 1. Choisir une stratégie

La mobilité et la consumérisation continuant à transformer radicalement l'informatique, plusieurs stratégies associent la liberté de choix à un contrôle accru des équipes informatiques :

- Le BYOD (Bring-your-own-device) : Permet aux collaborateurs d'utiliser leurs appareils personnels pour travailler.
- Le CYOD (Choose-your-own-device) : Permet aux collaborateurs de choisir un appareil appartenant à l'entreprise, à partir d'une liste limitée d'appareils autorisés à être utilisés à des fins professionnelles.
- Le COPE (Corporate-owned, personally enabled) : Permet aux collaborateurs de choisir un appareil appartenant à l'entreprise à partir d'une liste approuvée, et d'utiliser sur cet appareil aussi bien leurs propres applications que leurs applications d'entreprise.
- L'approche hybride : Une association des précédentes approches peut être adoptée dans le but de favoriser de la bonne manière la mobilité pour différents utilisateurs ou groupes d'utilisateurs. Le COPE peut par exemple être adopté parallèlement au CYOD ou au BYOD.



Si chacune de ces stratégies a ses propres spécificités, elles partagent toutes les principes fondamentaux de la gestion unifiée des terminaux (UEM), et notamment ses implications en matière de sécurité. C'est essentiellement le coût qui les différencie.

Les utilisateurs du BYOD payent leurs appareils et leurs abonnements, en bénéficiant parfois d'une allocation totale ou partielle versée par l'entreprise. Dans le cas du COPE et du CYOD, c'est l'entreprise qui paie directement l'appareil et les abonnements. En outre, les stratégies BYOD intègrent parfois des éléments qui dépassent le cadre des programmes COPE ou CYOD, comme la question de savoir si les collaborateurs doivent être rémunérés en heures supplémentaires lorsqu'ils consultent leur messagerie professionnelle en dehors des heures ouvrées et le week-end.

### 2. Admissibilité et enregistrement

Vous devez identifier clairement les personnes autorisées à utiliser des appareils personnels, que ce soit sur une base ponctuelle pour compléter un appareil d'entreprise, pour le remplacer de façon permanente ou pour tout autre cas de figure. Cela peut être considéré comme un privilège à gagner, une réponse à la demande d'un collaborateur, une exigence pour certains types de rôles, un risque excessif pour certains scénarios d'utilisation ou, plus vraisemblablement, une combinaison de tout cela.

Une façon de déterminer l'admissibilité consiste à appliquer des critères, tels que le type d'utilisateur, la fréquence des déplacements ou la nécessité pour cette personne d'accéder à des données sensibles hors ligne. Bien que les conditions d'admissibilité soient assez larges, les managers doivent avoir le dernier mot quant aux membres du personnel considérés comme étant des candidats appropriés à recevoir une allocation. Les managers peuvent également mettre en œuvre le BYOD, le CYOD ou le COPE dans le cadre d'autres incentives, privilèges et mesures disciplinaires au sein d'un service.

Les sous-traitants sont généralement les candidats au BYOD par excellence. De nombreuses entreprises s'attendent déjà à ce que les sous-traitants apportent leur propre appareil, et leur demander qu'ils le fassent contribue à la conformité des sous-traitants indépendants.

### 3. Appareils autorisés

Pour éviter une diversité ingérable d'appareils, vous pouvez limiter les types d'appareils mobiles pris en charge dans l'entreprise. La granularité de cette stratégie dépendra des besoins de vos utilisateurs, des risques encourus et de vos ressources de support technique disponibles. D'une manière générale, plus votre stratégie est détaillée en termes de types d'appareils, de versions de système d'exploitation et de numéros de modèles, plus les ressources nécessaires pour tester et maintenir de façon adéquate les appareils concernés devront être importantes.

Afin de clarifier les choses en matière de propriété, les participants au programme BYOD doivent être invités à acheter leur propre appareil en passant par les circuits de consommation normaux, plutôt qu'auprès du service achats de l'entreprise. Vous pouvez faire profiter vos collaborateurs de réductions, dans le cadre de vos accords avec des fournisseurs professionnels.

Certaines personnes peuvent également demander des équipements complémentaires, comme des écrans ou des claviers. Veillez dans ce cas à définir qui achète et possède chaque article.

### 4. Déploiement

La communication est essentielle à la réussite de votre déploiement. Offrez des conseils pour aider vos collaborateurs à décider s'ils souhaitent participer et comment choisir l'appareil correspondant à leurs besoins. Ils doivent également parfaitement comprendre comment accéder aux données, les utiliser et les stocker, et connaître la façon appropriée d'installer et d'utiliser à des fins professionnelles des comptes de services ou d'applications grand public non gérés par l'entreprise.

Les données professionnelles doivent être strictement séparées afin de respecter les exigences de e-Discovery et les politiques de stockage des données ; de la même façon, aucun email professionnel ne doit être envoyé depuis un compte personnel. La politique d'utilisation doit s'appliquer de la même façon aux appareils BYOD et aux appareils d'entreprise.

Il est également important de mettre en place un programme d'aide à l'adoption qui aidera les participants à devenir opérationnels rapidement. Un email de bienvenue contenant un lien vers un portail en libre-service peut aider les utilisateurs à devenir plus productifs, plus rapidement.

### 5. Partage des coûts

La réduction des coûts est l'un des principaux avantages du BYOD, puisque les collaborateurs prennent à leur charge tout ou une partie du coût des différents appareils personnels qu'ils utilisent pour travailler. Les entreprises qui attribuent une allocation prennent généralement en charge de 18 à 20 % du coût de l'appareil. Les participants doivent savoir que l'allocation est considérée comme un revenu d'un point de vue fiscal. Dans les pays où l'impôt sur le revenu est élevé, vous pouvez envisager d'augmenter l'allocation en fonction de cela afin que le montant net des subventions soit le même pour tous les participants.

Si vous choisissez d'offrir une subvention, celle-ci doit refléter l'intégralité de la participation de chaque personne. Les subventions doivent être renouvelées à intervalles réguliers afin de garantir que les appareils personnels ne dépassent pas l'âge attendu pour un appareil d'entreprise. Si un participant quitte l'entreprise pendant un cycle BYOD, vous pouvez réclamer une partie de l'allocation.

N'oubliez pas que le partage des coûts a des implications pour l'entreprise lorsque vous introduisez votre programme BYOD. Un déploiement en une seule fois peut augmenter les coûts lorsque les utilisateurs décident de participer au programme (et de réclamer leur allocation), et ce en tout point du cycle de rafraîchissement. Proposer le programme aux utilisateurs lorsqu'ils approchent de la fin de la durée de vie de leur appareil permet d'étaler l'impact. Au contraire, les entreprises ne proposant pas d'allocation peuvent inviter les utilisateurs à participer au programme dès sa mise en place.

De plus, toute stratégie BYOD, avec ou sans partage des coûts, doit identifier clairement qui paiera pour l'accès au réseau en dehors du pare-feu d'entreprise, que ce soit via un réseau mobile, un accès public à Internet sans fil ou une connexion haut débit à la maison.

### 6. Sécurité et conformité

Un prérequis essentiel demeure, que le propriétaire de l'appareil soit l'entreprise ou le collaborateur : la protection efficace des données sans impact négatif sur l'expérience. Pour les programmes autorisant la présence d'applications et de données personnelles sur les appareils utilisés à des fins professionnelles, la gestion des applications mobiles (MAM) permet d'assurer une séparation entre les contenus personnel et professionnel.

Installer des applications professionnelles sur des appareils personnels accroît les risques. Mais une stratégie combinant la gestion unifiée des terminaux, la virtualisation de postes et d'applications et le partage sécurisé des fichiers permet d'éviter d'avoir à le faire. Les données d'entreprise demeurent en sécurité dans votre datacenter ou dans le cloud. Dans les cas où les informations n'ont pas besoin de résider sur l'appareil mobile, les données d'entreprise peuvent être protégées via des mécanismes de création de conteneurs, de chiffrement et de suppression à distance. Vous pouvez également désactiver l'impression ou l'accès au stockage côté client (disques locaux, périphériques de stockage USB, etc.).

Vous pouvez contrôler et sécuriser l'accès aux données et aux applications à l'aide de stratégies basées sur le propriétaire de l'appareil, son statut et sa localisation. Enregistrez et gérez tout appareil, définissez des critères de création de mots de passe, détectez les appareils débridés et supprimez tout ou partie d'un appareil non conforme, perdu, volé ou appartenant à un employé ou un sous-traitant ayant quitté l'entreprise. Garantissez la sécurité des applications grâce à un accès sécurisé via des tunnels applicatifs, une liste d'applications autorisées et interdites, ainsi que des stratégies dynamiques en fonction du contexte.

Pour protéger le réseau de l'entreprise, vous pouvez utiliser une technologie de contrôle d'accès réseau (NAC), qui authentifie les utilisateurs se connectant au réseau et vérifie si leur appareil dispose d'un antivirus et de correctifs de sécurité à jour.

En dehors du pare-feu, la virtualisation et le chiffrement peuvent dissiper la plupart des failles sécuritaires associées au Wi-Fi, au chiffrement WEP, à la connectivité sans fil ouverte, à la 3G/4G et aux méthodes d'accès grand public. Les fonctionnalités de sécurité réseau offrent

non seulement visibilité et protection contre les menaces mobiles internes et externes, en bloquant les appareils malveillants, les utilisateurs non autorisés et les applications non conformes, mais aussi l'intégration de systèmes de gestion du système d'information (SIEM).

En cas de départ d'un participant au programme BYOD, d'une violation de la stratégie correspondante, de perte ou de vol d'un appareil personnel, l'équipe informatique doit disposer d'un mécanisme pour résilier instantanément l'accès aux données et aux applications, notamment pour déprovisionner les comptes SaaS professionnels et supprimer à distance les données présentes sur les appareils égarés. Cette fonctionnalité est également essentielle pour les appareils CYOD ou COPE, car elle permet de réattribuer un appareil d'entreprise à un nouvel utilisateur sans que les données laissées sur celui-ci ne tombent entre les mains d'un utilisateur non autorisé à y accéder.

Plutôt que d'adopter une approche BYOD ouverte, permettant aux utilisateurs d'apporter n'importe quel appareil pour accéder aux données et applications d'entreprise, certaines entreprises optent pour une approche managée. Dans ce cas de figure, la direction informatique gère directement l'appareil personnel, y compris son enregistrement, sa validation, ses autorisations et son accès aux ressources.

### 7. Gestion et supervision

La gestion et la supervision quotidiennes sont essentielles pour garantir la conformité des stratégies et garantir le retour sur investissement.

Certaines solutions UEM améliorent l'efficacité et la productivité informatiques en automatisant différents aspects de la gestion et de la supervision. Par exemple, la définition des actions précises à entreprendre en cas de violations diverses. Ces actions peuvent notamment inclure la suppression totale ou partielle de l'appareil, la qualification de l'appareil comme non conforme, la révocation de l'appareil ou l'envoi d'une notification à l'utilisateur lui enjoignant de corriger un problème (supprimer une application interdite, par exemple) dans un certain délai avant que des mesures plus sévères ne soient appliquées.

### 8. Support et maintenance des appareils

Un programme BYOD réduit souvent la maintenance informatique nécessaire pour chaque appareil, car l'utilisateur en est également le propriétaire. Cela dit, la stratégie doit préciser clairement la façon dont les activités de support et de maintenance doivent être gérées et payées, afin d'éviter une complexité et des tâches accrues pour l'IT. Dans le cadre de la plupart des programmes CYOD ou COPE, la direction informatique est entièrement responsable du support et de la maintenance des appareils.

## Comment Citrix Workspace permet une gestion sécurisée des appareils

Tout programme de gestion des appareils doit intégrer des technologies qui garantissent l'accès sécurisé aux applications et fichiers d'entreprise depuis les appareils personnels. Citrix Workspace offre toutes les fonctionnalités clés nécessaires pour rendre le BYOD, le CYOD ou le COPE simple, sûr et efficace pour toute entreprise. Cette solution associe la gestion unifiée des terminaux, la virtualisation des postes et applications Windows, le partage sécurisé de fichiers et la mise à disposition d'applications pour vous permettre de mettre à disposition vos applications et données d'entreprise sur tout appareil utilisé à des fins professionnelles par vos collaborateurs, tout en préservant la sécurité et le contrôle.

### Gestion unifiée des terminaux

Bénéficiez de fonctionnalités de provisioning et de contrôle des applications, des données et des appareils basés sur l'identité, de suppression de compte automatique pour les utilisateurs ayant quitté l'entreprise et de suppression sélective sur les appareils égarés. Citrix Workspace vous permet non seulement de gérer les appareils (y compris IoT), mais également de garantir la sécurité et le contrôle au niveau des applications, pour protéger vos données d'entreprise sans impacter l'utilisation des contenus personnels sur les appareils BYOD, CYOD ou COPE. La gestion des terminaux de Citrix Workspace vous permet de définir quelle stratégie MAM est la plus adaptée à vos besoins, qu'il s'agisse d'une plateforme MAM de type Samsung KNOX ou Appconfig, de Citrix MDX (qui fournit une couche supplémentaire de chiffrement applicatif sans enregistrement des appareils) ou d'Intune MAM.

### Virtualisation de postes et d'applications Windows

Au lieu d'installer et de gérer individuellement des applications et des postes Windows sur chaque appareil, vous pouvez les mettre à disposition sous forme de services à la demande sur tout appareil. Les applications et les données étant gérées dans un datacenter, l'équipe informatique assure la protection des données, la conformité, le contrôle d'accès et l'administration des utilisateurs de façon centralisée, aussi facilement sur des appareils personnels que sur des appareils d'entreprise, le tout dans un environnement unifié.

### App store

Offrez à vos collaborateurs un accès en un clic aux applications mobiles, web, SaaS, d'entreprise et Windows, via un app store unifié. Peu importe l'appareil choisi (ordinateur Windows ou Mac, iOS, Android, produit mobile Windows ou Google Chromebook), l'expérience utilisateur sera la même, quels que soient l'appareil, le lieu et le réseau.

### Accès sécurisé

Un cadre de gestion unifié permet à l'équipe informatique de sécuriser, de contrôler et d'optimiser l'accès aux applications, aux postes de travail et aux services sur tout appareil. Des fonctionnalités d'audit et de création de rapports favorisent en outre la conformité et la protection des données. Seul Citrix propose un micro-VPN sans égal, qui renforce la protection des données d'application entre l'appareil mobile et les ressources d'entreprise, derrière le pare-feu.

### Partage de fichiers sécurisé

Les personnes peuvent partager des fichiers aisément et en toute sécurité avec n'importe qui au sein de l'entreprise ou à l'extérieur, et synchroniser leurs fichiers sur tous leurs appareils. Le contrôle d'accès basé sur des stratégies, l'audit, la création de rapports et la suppression à distance de l'appareil contribuent à sécuriser le contenu de l'entreprise.

En adoptant les bonnes stratégies et technologies, vous assurez l'équilibre parfait entre d'une part la liberté de choix de vos collaborateurs et d'autre part la sécurité et le contrôle de votre IT. Pour découvrir dans quelle mesure Citrix Workspace peut vous aider à rendre la gestion des appareils simple et sécurisée, consultez www.citrix.fr/workspace

**Ventes aux entreprises**
Amérique du Nord | 800 424 8749
International | + 1 408 790 8000

**Sites**
Siège social | 851 Cypress Creek Road Fort Lauderdale, FL 33309, États-Unis
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, États-Unis