



# Politique de sécurité pour PDA

MARS 1, 2005

ADONIS AKA NTWAKO @ SAFEHACK.COM

## Introduction

À la différence des logiciels d'exploitation, nous n'avons pas trouvé ce que sont les menaces à ces nouveaux dispositifs puissants les PDA. Pire, ces logiciels d'exploitation minuscules inclus actuellement peu ou pas de sécurité. Les dispositifs PDA font partie de notre vie quotidienne, il faut donc comprendre la sécurité derrière ces bidules.

Ce document décrit la politique admise d'utilisation liée aux dispositifs (PDA) personnels.

## Définition Assistant numérique personnel (PDA)

Le PDA est un dispositif à main qui combine l'ordinateur, le téléphone et des caractéristiques de réseautage. Un modèle de base comprend les applications suivantes : tablette électronique, carnet d'adresses, calendrier et autres. Avec un modèle de pointe, il est possible d'envoyer et de recevoir des courriels, de faire du traitement de texte; d'écouter des fichiers de musique MP3, de jouer à des jeux vidéo et d'avoir une appareil-photo numérique intégré ou un récepteur GPS. Certains modèles comprennent également un téléphone numérique.

<http://www.apt.gc.ca/dProdExpandF.asp?Id=412>

## C'est quoi une politique de sécurité et pourquoi elle est nécessaire ?

Une politique de sécurité peut être définie comme des règles ou lois spécifiques qui sont mises en place pour assurer la sécurité d'information.

La plupart des pays ont des lois qui concernent la vie privée de ses citoyens ; ces lois sont un facteur dans les politiques de sécurité.

D'autres facteurs sont la sensibilité de l'information, sécurité nationale et sécurité personnelle. Les bonnes politiques de sécurité adressent tous ces facteurs.

Les politiques de sécurité sont également essentielles pour l'assurance (dans certain cas). Les grands assureurs comptent qu'une compagnie aura fait son meilleur pour éviter un incident. Les politiques de sécurité sont nécessaires pour prouver ceci, de la même manière compagnies d'assurance s'attendent à ce que vous fermez votre porte à la avant de partir.

La responsabilité finale se trouve avec le CEO de n'importe quelle compagnie. Son travail doit s'assurer que la politique de sécurité est écrite professionnellement. Le CEO ne doit pas écrire la politique, mais lui ou elle doit assurer la qualité de la politique.

L'officier de sécurité devrait également avoir beaucoup à dire dans la politique, car son travail est d'être

entièrement familier avec les systèmes d'information de l'organisation.

Les politiques exigent la planification et la recherche avant qu'elles puissent être mises en application.

Quel type de politique sera mis en application dans votre organisation ?

**C'est important de considérer les facteurs suivants :**

**Menaces** : Quelles sont les menaces potentielles ou le champ mobile que vous voulez protéger ? Une menace est quelque chose qui a le potentiel d'endommager. Ce peut être une activité par un utilisateur ou un événement tel qu'une infection par un virus.

**Vulnérabilités** : Est ce que le champ mobile que vous essayez protéger as des failles qui permettraient une attaque interne ou externe ? Les vulnérabilités constituent une menace importante.

**Risque** : Un risque peut être décrit comme probabilité de l'occurrence d'une menace et les dommages soutenus par un individu ou une compagnie, financière ou autrement, due à cette menace. Il est important de différencier entre les menaces probables et les menaces peu probables.

Les dispositifs mobiles ont révolutionné la façon que des affaires entre les gens. Les mobil-phones en particulier deviennent de plus en plus communs, non seulement pour des utilisateurs d'affaires mais pour tout le monde.

Avec les avances accrues en technologie viennent également les plus grands risques et des menaces à l'information qui est stockée et ou traversent ces dispositifs.

Avec l'apparition du *malware* pour les dispositifs mobiles, les compagnies sont forcées de mettre en place des politiques de sécurité pour les *PDA*s.

Les politiques efficaces s'assureront que la confidentialité, l'intégrité et la disponibilité sont maintenues.

**Exécution** : Que doit être sécurisé ?

En premier lieu le dispositif doit être sécurisé physiquement. Le vol et la perte jouent un facteur important dans les infractions des dispositifs mobiles. Le remplacement d'un dispositif volé ou perdu n'est pas bon marché ; d'une manière primordiale, les données sur un dispositif peuvent être irremplaçables, et la politique de sécurité doit refléter ceci.

La petite taille des dispositifs leur fait des cibles faciles pour des voleurs. Le PC de poche peut facilement être enlevé sans beaucoup d'effort. Mal placer un dispositif est également relativement facile.

La société PointSec ont conduit une recherche et qui ont soulevées des résultats étonnants. A Chicago (Etats-Unis), pendant les 6 mois de l'étude, 85.619 mobilophones, 21.460 *PDA*s/Pocket, et 4.425 ordinateurs portatifs ont été oubliés dans des taxis.

<http://www.pointsec.com/news/release.cfm?PressId=44>

Les employés doivent être jugés responsables de leur dispositif. Les accidents peuvent et se produisent, mais la perte peut être réduite au minimum quand le personnel sont encouragés à prendre la propriété de leur dispositif. Le stockage physique approprié d'un dispositif inutilisé doit être adressé également.

Tous les types du stockage, démontable ou d'autre doivent être protégés.

Les cartes "SD" ont la capacité d'emmagasiner des gigaoctets des données et elles sont la taille d'un timbre-poste. Les données sur ces dispositifs sont également vulnérables et peuvent etre endommager par la chaleur, des radiations "RFI" et des dommages électro magnétiques. Ceci doit être adressé.

Les protocoles pour le transfert de données doivent être sécurisés.

## Mécanismes de contrôle d'accès.

L'utilisation des mécanismes de contrôle d'accès dans votre parc des dispositifs mobiles est essentielle pour empêcher l'accès non autorisé des données. Le contrôle d'accès doit être fort et bien examiné.

Les procédés d'authentification doivent être faciles à utiliser et le temps d'authentification doit être court. Les utilisateurs ne sont pas intéressés par la sécurité ; ils veulent seulement pouvoir accéder à leur travail facilement. Si le processus prend du temps ou difficile vous pouvez constater que les employés rechercheront des manières pour neutraliser les mécanismes de contrôle d'accès.

Beaucoup de mobile-phones ont des fonctions de mise au point dure codée dans le dispositif. Les voleurs peuvent employer ces codes pour dévier les mesures d'authentification et pour accéder aux données protégées. Essentiellement c'est comme une porte arrière qui donne accès aux données stockées sur le dispositif.

## Chiffrage

Même si un attaquant parvient à casser un système de contrôle d'accès, les données correctement chiffrées ne seront pas utiles.

Comme avec les mécanismes de contrôle d'accès, il est important de s'assurer qu'il n'est pas difficile pour que l'utilisateur emploie le procédé de chiffrage.

Des mots de passe et les passphrases devraient être gardés séparé du dispositif, la formation du personnel aidera à assurer ceci.

Quelques sociétés placent des backdoors cachés dans leur logiciel de chiffrage. Un facteur important à se rappeler lorsque vous achetez des logiciels de chiffrage, les compagnies qui n'est pas bien établie, elles ne sont pas recommandées.

## Firewall et IDS

Juste comme une machine de bureau, les dispositifs mobiles sont également vulnérables aux attaques et aux intrusions à distance. Un pare-feu approprié protégera non seulement le dispositif d'utilisateurs, mais également protégera n'importe quel réseau de corporation auquel ce dispositif a accès.

Un dispositif non protégé est littéralement une porte secrète pour votre réseau. Les configurations des firewalls doivent être facilement administrées et les paramètres obligatoires doivent être entièrement transparents. Il ne faut pas permettre les employés d'accéder aux paramètres du pare-feu. Il est également préférable que les "rulesets" du pare-feu soient mis à jour régulièrement.

Le logiciel d'IDS n'est pas commun sur les dispositifs mobiles, mais il y a quelques produits autour. Les bonnes logicielles identifications peuvent aider un administrateur quand il veut debugger un dispositif mobile.

## Protection contre les virus et les Malwares

Des dispositifs mobiles sont activement visés par les programmeurs des virus. La gamme du logiciel disponible pour les dispositifs mobiles change mais il devrait être facile à utiliser.

Des configurations obligatoires devraient être imposées de sorte que les utilisateurs ne puissent pas neutraliser le logiciel d'antivirus. Le logiciel devrait être facilement mis à jour. Le logiciel d'Antivirus ne devrait pas essayer et détecter les virus qui ne visent pas les dispositifs mobiles.

## Effacement de données

Le logiciel d'effacement de données est exigé pour tous les dispositifs qui manipulent l'information confidentielle. Ce logiciel devrait au moins rencontrer les directives du département de la défense USA. Standard DoD [www.dss.mil](http://www.dss.mil). Ce type de sécurité protégera les vieilles données.

L'effacement de données devrait également être commandé de telle sorte que les utilisateurs n'effacent pas accidentellement l'information importante. Ceci peut être adressé avec des configurations restrictives aussi bien qu'avec la formation du personnel. Le logiciel devrait également demander à un utilisateur au moins une fois s'ils veulent vraiment effacer l'information. Il faut examiner avec un logiciel approprié pour vous assurer que l'information ou les données ont été effacées.

## Synchronisation

Quand un dispositif est synchronisé avec un ordinateur au lieu de travail il est essentiel que des mesures soient mises en place pour arrêter le dispositif de rechercher les documents confidentiels.

Le logiciel de synchronisation permettra au dispositif de saisir tous les nouveaux documents sans vérifier s'ils sont confidentiels ou pas. Le problème se produit quand un employé prend son dispositif à la maison et synchroniser avec leur ordinateur personnel.

Les documents confidentiels sont maintenant transférés à la machine à la maison de l'utilisateur, qui peut ne pas avoir les mécanismes de sécurité en place que les ordinateurs de la compagnie. La synchronisation automatique silencieuse de wifi devrait être désactivée. Si un dispositif peut synchroniser avec un ordinateur erroné.

## Formation du personnel

La formation du personnel est un aspect essentiel de toute bonne politique. Rendre vos expériences de formation agréables, ne pas surcharger le personnel avec le jargon fortement technique.

La formation du personnel appropriée est également la meilleure assurance contre l'ignorance des mesures de sécurité. Si cet employé a été montré quoi faire, alors la responsabilité est sur elles en cas d'une infraction ou un incident de sécurité se produira. Des directives strictes de la politique devraient être disponibles aux personnels. Ces politiques devraient être imposées en utilisant un système des avertissements. Le nouveau personnel peut faire une équipe avec d'autre personnel responsable duquel ils peuvent apprendre. Le personnel devrait être récompensé pour une bonne pratique.

## Configuration obligatoires de dispositif

Tous les dispositifs dans votre flotte mobile devraient avoir en place des configurations obligatoires qui sont impossibles à changer par l'utilisateur moyen. Si le dispositif n'a pas besoin d'avoir un "wifi", alors ceci devrait être désactivé, la même chose s'applique au Bluetooth et infrarouge.

Si vos employés n'ont aucune raison de jouer des fichiers type médias tels que mp3s, mpgs, et d'autre? Alors je vous recommande de supprimer le logiciel qui aide à jouer ce type des fichiers. Des virus a été trouvés dans les logiciels piratés pour les dispositifs mobiles. Il est impératif que les employés soient entièrement instruits sur le risque impliqué en installant ce type de logiciel.

## Manque de se conformer à la politique

Pour la première violation de cette politique, le propriétaire de PDA sera donné un avertissement par écrit de leur infraction, et soit prié de lire et reconnaître la politique de PDA en signant une copie de la politique, qui sera placée dans leur dossier administratif.

Si une deuxième violation se produit, le propriétaire du PDA sera donné un deuxième avertissement par écrit, et invité à rendre le PDA à la compagnie si le PDA est la propriété de la compagnie. Toute autre violation de cette politique aura comme conséquence l'arrêt du travail.

## Directives pour la politique

Un PDA peut stocker des données dans la mémoire persistante, le stockage externe (exemple: flash, SD), ou la RAM interne.

**RAM interne** - toutes les données sensibles en service doivent être stockées dans la présente partie de la mémoire durant le processus de déchiffrement.

**Mémoire persistante** - la présente partie de mémoire maintient son statut durant une perte de puissance, ce qui élimine le besoin de réinstallation s'il y a une perte de puissance. Les propriétaires de PDA peuvent installer leurs applications dans cette section de mémoire, aussi longtemps qu'aucune donnée sensible n'est stockée dans les annuaires de programme.

**Mémoire externe** - la mémoire externe doit être utilisée seulement pour les données qui n'ont aucun risque de sécurité (musique, jeux). Si les données sont chiffrées selon les conditions de la politique de la sécurité, alors cette section de la mémoire peut être utilisée pour stocker cette information, ceci inclut les fichiers de sauvegarde chiffrés.

**Utilisation avec réseau (Email/Autre.)** - Le PDA peut être utilisé pour accéder à des serveurs web et cela n'est pas un risque de sécurité. Le courriel peut être téléchargé au PDA avec un lien sécuritaire. Le lien de sécurité devrait se composer d'un VPN ou par l'intermédiaire d'une connexion SSL.

**Authentification et identification** - chaque dispositif PDA doit être protégé par un mot de passe. Le mot de passe doit contenir des lettres et des nombres. En outre, il doit y avoir un contrôle en place pour empêcher les attaques par force brutale.

**La perte (perdu ou volé)** - Si un PDA est perdu ou volé, le propriétaire doit immédiatement entrer en contact avec le département "IT" et rapporter l'incident. Un inventaire des programmes et des données doit également être inclus avec le rapport.

**Applications tiers partie** - seulement des applications approuvées peuvent être installées sur les PDAs.

**Synchronisation** - la synchronisation du PDA au PC peut seulement se produire localement ou par l'intermédiaire d'un lien sécuritaire.

**VPN** - Un VPN est exigé pour relier le PDA à l'environnement de la corporation de l'extérieur. Ceci inclut le courriel à distance, la synchro à distance, et d'autre.

**Chiffrement** - le logiciel de chiffrement devrait se conformer aux algorithmes cryptographiques forts actuellement admis. Le programme de chiffrement devrait inclure une méthode pour effacer les données d'une façon sécuritaire.

**Pare-feu** - Un pare-feu personnel géré par le système central est obligatoire sur tout les PDAs.

**Antivirus** - Les programmes pour balayer les virus doivent être mis à jour régulièrement.

Adonis a.K.a NtWaK0, Eng, CISSP, CEH Certified Ethical Hacker, GSec, MCSE

[www.safehack.com](http://www.safehack.com)