Ligne directrice sécurité de l'information & vie privée :

Appareils mobiles

(BLD MOBILE)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

L'usage d'appareils mobiles à des fins professionnelles est soumis à une série de mesures de contrôle. Toute organisation doit prendre les mesures appropriées en matière de sécurité de l'information et de vie privée pour se protéger contre les risques liés à l'usage d'appareils mobiles tels

- la perte d'informations sensibles due
  - au vol ou à la perte de l'appareil mobile
  - à la simplicité des mots de passe ou combinaisons de chiffres
  - à l'absence de contrôle d'accès à l'appareil mobile
- la divulgation non intentionnelle de données sensibles
- les attaques par des codes malveillants tels les malware, spyware, ransomware, ...
- les attaques liées à l'utilisation d'internet ou de l'e-mail telles que le phishing
- les attaques provenant de réseaux sans fil non sécurisés

La politique s'applique tant aux appareils mobiles mis à la disposition par l'organisation qu'aux appareils mobiles privés.

2. Utilisation sécurisée d'appareils mobiles

Toute organisation souscrit la politique suivante relative à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation.

La présente politique est liée à la politique relative à la gestion centrale et à l'inventorisation des appareils. Les présentes directives doivent être rédigées, validées, appliquées par l'organisation et communiquées à l'ensemble des parties concernées. Les présentes directives s'appliquent à l'ensemble des utilisateurs qui ont accès aux informations de l'organisation au moyen d'appareils mobiles[1].

a. Toute organisation doit prendre les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles ne soient accessibles qu'aux seules personnes autorisées.

b. Toute organisation doit prendre les mesures adéquates, en fonction du moyen d'accès[2], afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation.

c. L'utilisation d'appareils privés à des fins professionnelles ne peut être envisagée qu'aux conditions suivantes :

   1) Les conditions d'utilisation doivent être définies sur la base d'une évaluation des risques qui tient compte des besoins légitimes (notamment des données utilisées) et des circonstances d'utilisation.

   2) L'organisation doit offrir suffisamment de garanties que les appareils mobiles privés satisfont à un niveau de sécurité de l'information et de vie privée comparable à celui dont les appareils mobiles de l'organisation sont équipés.

[1] Par « appareils mobiles », on entend dans un premier temps les smartphones et tablettes utilisant un système d'exploitation mobile tel que Google Android, Apple iOS, Microsoft Windows, etc. Toutefois, le terme « appareil mobile » désigne aussi les netbooks et autres appareils pouvant être utilisés en dehors de l'organisation.

2 Moyen d'accès: p.ex. Internet, ligne louée, réseau privé, réseau sans fil.

3) L'organisation garantit que l'accès aux données de l'organisation au moyen d'un appareil mobile est uniquement possible selon le principe suivant: « Afin de garantir la sécurité de l'information et la vie privée des données de l'organisation, le niveau requis sera toujours proportionnel à la nature et à la sensibilité des données ».

4) L'appareil mobile privé de l'utilisateur final doit être géré par l'organisation.[3]

5) Un contrat d'utilisation doit être conclu entre l'utilisateur et l'organisation pour ce qui concerne l'usage professionnel de l'appareil mobile. Par la signature du contrat d'utilisation, l'utilisateur déclare être d'accord avec les directives et devient responsable pour l'utilisation de l'appareil mobile.

d. Si les appareils mobiles peuvent être utilisés à des fins professionnelles et à des fins privées, l'utilisateur doit respecter les règles relatives à la sécurité de l'information et à la vie privée qui ont été rédigées par l'organisation.

1) L'utilisateur doit demeurer vigilant lorsqu'il utilise l'appareil mobile à des fins privées, et ce conformément aux présentes directives et aux directives spécifiques en matière de sécurité de l'information et de vie privée.

2) L'utilisateur est le seul responsable de l'utilisation de l'appareil mobile. L'utilisateur est conscient des risques liés aux appareils mobiles, surtout lorsqu'il se connecte au système d'information de l'organisation. C'est pourquoi il s'engage à respecter les règles relatives à la sécurité de l'information afin d'éviter tout abus, perte ou vol.

3) En cas de perte ou de vol, l'utilisateur avertit immédiatement le service compétent de l'organisation. Il en va de même pour un appareil mobile privé utilisé à des fins professionnelles.

e. L'organisation identifiera clairement les appareils mobiles propres, les configurera en toute sécurité (et les équipera des logiciels antimalware nécessaires ainsi que des logiciels permettant la suppression à distance de l'ensemble des données sur l'appareil) et conservera leur identification dans un registre central.

f. L'organisation peut vérifier la conformité des appareils mobiles aux directives relatives à la sécurité de l'information et à la vie privée (à distance au moyen d'un logiciel ou sur place au moyen d'un contrôle direct), afin de limiter les risques à un niveau acceptable, et ce conformément aux attentes de l'organisation. Afin de garantir le niveau, l'organisation doit mettre en place les mesures adéquates[4]. L'organisation n'est pas responsable pour les dommages ou frais qu'entraîne la perte ou le vol de données privées.

g. L'organisation s'engage à sensibiliser régulièrement les utilisateurs concernant les bonnes pratiques d'utilisation et leurs responsabilités (en particulier en ce qui concerne la connexion à des réseaux sans fil publics).

h. L'organisation disposera toujours de la possibilité de bloquer directement l'accès aux informations de l'organisation (données ou applications présentes sur l'appareil mobile) et d'effacer des données.

i. L'organisation s'engage à respecter la vie privée de l'utilisateur.

[3] Si l'appareil mobile permet une séparation logique entre l'environnement professionnel et l'environnement privé, le contrôle sera limité à l'environnement professionnel.

[4] Toujours sur la base d'un accord réciproque entre l'organisation et l'utilisateur.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2003		V2003	Première version	10/09/2003	01/10/2003
2004		V2004	Deuxième version	11/02/2004	01/12/2004
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, septembre 2013, 23 p.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, septembre 2013, 80 p.
- ISACA, “COBIT 5 for Information Security”, mai 2012, 220 p.
- ISACA, “Mobile computing security audit/assurance program”, octobre 2010, 23 p.
- ENISA, “Smartphone security development guidelines”, decembre 2016, 28 p.
- NIST, “Guidelines for managing the security of mobile devices in the enterprise”, juin 2013, 30 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.isaca.org/cobit
- http://ccb.belgium.be/nl/guidelines
- https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Annexe C: directives pour l'usage sécurisé d'appareils mobiles

Ci-après figurent plusieurs directives pour l'organisation afin d'utiliser les appareils mobiles en toute sécurité.

1. Le niveau de la sécurité de l'information et de la vie privée requis pour les appareils mobiles dépend de la nature et de la sensibilité des données. Les tableaux ci-dessous contiennent un aperçu des directives à appliquer en fonction des trois modèles techniques envisageables pour la gestion des appareils mobiles.

A. Modèles techniques de gestion en fonction de la classification des données

Classification des données	Exemple	Dispositif mobile sans gestion centralisée	Dispositif mobile avec gestion centralisée	Dispositif mobile avec environnements distincts (isolation[5]/VDI[6])
Données publiques	Site web BCSS, site web ONSS	oui	oui	oui
Données internes de l'entreprise	Stratégie interne, agenda, contacts, mails	À déterminer[7]	oui	oui
Données confidentielles de l'entreprise	Plan comptable, plan de continuité	non	À déterminer	oui
Données à caractère personnel	Dossier personnel HR	non	À déterminer	oui
Données sociales à caractère personnel	Données registre national	non	non	oui
Données médicales	Données médicales	non	non	oui

B. Mesures de sécurité en fonction du modèle de gestion

Mise en œuvre obligatoire de mesures de sécurité	Dispositif mobile sans gestion centralisée	Dispositif mobile avec gestion centralisée	Dispositif mobile environnements distincts (isolation/VDI)
Sensibilisation et responsabilisation	oui	oui	oui
Système d'authentification des utilisateurs sur le dispositif	Recommandé	oui	oui
Verrouillage de l'appareil en cas d'inactivité	Recommandé	oui	oui
Politique des mots de passe	Recommandé	oui	oui
Blocage automatique après l'introduction de X codes d'accès erronés	non	oui	oui
Communication sécurisée pour l'accès aux informations de l'entreprise	oui	oui	oui
Authentification forte pour l'accès aux informations de l'entreprise	Recommandé	oui	oui
Contrôle de la présence d'un logiciel antimalware	Recommandé	oui	oui

[5] Isolation: solution permettant de créer des environnements strictement distincts (professionnel et privé) sur un appareil mobile. Seule la partie professionnelle tombe sous le contrôle de l'employeur

[6] Virtual Device Interface: *thin client* installé sur un support mobile permettant de travailler à distance via une session sécurisée dans un environnement professionnel.

[7] La notion « à déterminer » signifie que l'institution fixe le set de données qui est accessible sur base des trois modèles de gestion

Mise en œuvre obligatoire de mesures de sécurité	Dispositif mobile sans gestion centralisée	Dispositif mobile avec gestion centralisée	Dispositif mobile environnements distincts (isolation/VDI)
actif			
Contrôle de la dernière mise à jour du logiciel antimalware	non	oui	oui
Contrôle du niveau d'OS autorisé	non	oui	oui
Uniquement autoriser l'installation d'applications d'une source fiable	Recommandé	Recommandé	Recommandé / oui dans l'environnement de l'organisation
Limitation de la connectivité lors de l'accès aux informations de l'entreprise[8]	Recommandé	oui	oui
Chiffrement des données sur l'appareil	Recommandé	Recommandé	Le chiffrement est uniquement nécessaire en cas d'isolation
Blocage à distance	non	oui	oui
Suppression des données à distance	non	oui	oui, dans l'environnement de l'appareil mobile réservé à l'organisation
Notez le numéro IMEI de l'appareil	Recommandé	Recommandé	Recommandé

2. L'utilisateur ne modifiera pas les paramètres relatifs à la sécurité de l'information et à la vie privée, même si cela est techniquement possible. L'utilisateur ne « rootera » ou « jailbreakera » pas l'appareil mobile[9].
3. L'utilisateur est averti lorsque l'appareil mobile n'est pas conforme aux normes minimales relatives à la sécurité de l'information et à la vie privée.
4. Si l'appareil mobile n'est pas conforme, l'accès aux informations de l'organisation est refusé.
5. En cas de perte ou de vol, l'appareil est verrouillé et, si cela est possible et s'avère nécessaire, les données sont effacées. Ce qui peut donner lieu à la perte de données personnelles enregistrées sur l'appareil mobile.

[8] La connexion internet n'est pas autorisée.

[9] Rooter est le terme permettant au propriétaire de l'appareil d'accéder, généralement en dehors de la procédure normale, à la gestion complète d'un ordinateur, smartphone, etc. De nombreux appareils utilisent une variante du système d'exploitation Unix dans lequel le « superuser » (gestionnaire) est désigné à l'aide du terme « root ». Rooter signifie dans ce cas accéder au compte « root » de l'appareil, alors que le fabricant de l'appareil ne le permet pas. Afin de tout de même y accéder, généralement à l'encontre de l'objectif du fabricant, il est généralement fait usage d'erreurs dans la protection du système d'exploitation. Pour certains systèmes d'exploitation, le terme « jailbreak » est plus courant: l'utilisateur est pour ainsi dire enfermé dans le système d'exploitation et essaie d'y échapper.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	**Oui**
Gestion des actifs	
Protection de l'accès	
Cryptographie	**Oui**
Protection physique et protection de l'environnement	
Protection des processus	
Sécurité de la communication	**Oui**
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****