O RGANISATIONNEL
C OMPORTEMENTAL

Utiliser des appareils nomades de façon sécurisée

fiche **11**

Si les appareils nomades sont appréciés et utiles parce qu'ils simplifient souvent les tâches quotidiennes des acteurs économiques, leur usage expose cependant l'établissement et ses partenaires à des risques nouveaux de perte ou de captation d'informations stratégiques qu'il est nécessaire de bien maitriser en prenant certaine précautions élémentaires.

O

- Veiller à ce que personne dans l'établissement n'utilise son appareil nomade personnel (ordinateurs portables, *smartphones*, tablettes, lecteurs MP3, etc.) à des fins professionnelles. Cette règle est souvent perçue comme une contrainte forte, notamment par l'encadrement supérieur ; elle est cependant d'une importance particulière.
- Proscrire toute politique de **BYOD** (*Bring your Own Device*) au sein de l'établissement.

C

- Désactiver la connexion automatique des appareils nomades aux points d'accès WiFi ouverts.
- Désactiver le Bluetooth lorsqu'il n'est pas utilisé.
- En plus du code PIN protégeant la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès à son *smartphone* ou à sa tablette et les configurer pour qu'ils se verrouillent automatiquement après un court moment d'inactivité.
- Activer le **chiffrement** des supports de stockage, lorsque cela est possible, ou chiffrer les données les plus sensibles à l'aide d'un logiciel dédié.
- N'installer que les applications nécessaires et vérifier à quelles données elles permettent l'accès avant de les télécharger sur l'appareil nomade (informations géographiques, contacts, appels téléphoniques, etc.). Éviter d'installer les applications demandant l'accès à des données qui ne sont pas strictement nécessaires au fonctionnement de l'appareil nomade.
- Effectuer des sauvegardes régulières des contenus sur un support externe pour pouvoir les conserver en cas de restauration de l'appareil dans son état initial.
- Être très attentif à ne pas se séparer des appareils nomades qui peuvent contenir des informations sensibles ou permettre d'accéder au réseau de l'établissement.

MOTS-CLÉS

BYOD ou **AVEC :**
Bring your Own Device ou « Apporter votre équipement personnel de communication ». Politique d'établissement qui admet ou préconise l'utilisation d'équipements de communication personnels à des fins professionnelles.

Chiffrement :
procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

POUR ALLER PLUS LOIN

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Utiliser des appareils nomades de façon sécurisée

RÉFÉRENT

- ANSSI