

## E4. Sécuriser le télétravail

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

### ORGANISATIONNEL

- Penser une politique de mise à disposition d'outils nomades maîtrisée afin d'éviter les écueils d'un recours au BYOD (*Bring your Own Device*) non contrôlé.
- Veiller à ce que personne dans l'entreprise n'utilise son appareil nomade personnel (ordinateurs portables, smartphones, tablettes) à des fins professionnelles, sans accord ni contrôle. Cette règle est souvent perçue comme une contrainte forte, notamment par l'encadrement supérieur ; elle est cependant d'une importance particulière.

### COMPORTEMENTAL

- 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 au smartphone ou à la tablette et les configurer pour qu'ils se verrouillent automatiquement après un court moment d'inactivité.
- Chiffrer les données les plus sensibles à l'aide d'un logiciel ou d'une application 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'entreprise.

## Mots clés

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

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

### Pour aller plus loin

- Agence nationale de la sécurité des systèmes d'information (Anssi)
  - [Guide des bonnes pratiques de l'informatique](#)
  - [Guide d'hygiène informatique](#)
  - [Recommandations de sécurité relatives aux mots de passe](#)
  - [Liste de logiciels de chiffrement que vous pouvez utiliser en toute confiance](#)
  - [Passeport de conseils aux voyageurs](#)
- Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance.