Terminaux utilisateur

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

**5.1 Terminaux utilisateur**

**5.2 Responsabilité d’utilisateur**

**5.3 Utilisation d’appareils personnels**

**5.4 Connexions sans fil**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de protéger l’information contre les risques introduits par l'utilisation des terminaux utilisateur.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Terminaux utilisateur » s’applique à l’ensemble du personnel ayant accès à des terminaux de l’organisation.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

USB – *universal serial bus* (bus série universel)

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Terminaux utilisateur

Activités de surveillance

Registre de la configuration

Sécurité des appareils mobiles

Protection de la vie privée

Propriété intellectuelle

Connexion sans fil

**4. Exigences de la norme ISO 27001 : 2022**

A.8.1 Terminaux utilisateur

Les informations stockées, traitées ou accessibles via un terminal utilisateur, doivent être protégée.

**5. Déroulement**

**5.1 Terminaux utilisateur**

La politique Terminaux utilisateur précise la configuration et la gestion sécurisées des terminaux utilisateur. La politique est communiquée à l’ensemble du personnel concerné et tient compte des éléments suivants :

* le type d'information et le niveau de classification que les terminaux utilisateur peuvent gérer, traiter, stocker ou prendre en charge
* l’enregistrement des terminaux utilisateur
* les exigences de protection physique
* la restriction de l'installation du logiciel (contrôle à distance par les administrateurs système)
* les exigences relatives au logiciel du terminal utilisateur (y compris les versions logicielles) et à l'application des mises à jour (mise à jour automatique active)
* les règles de connexion aux services d'information, aux réseaux publics ou à tout autre réseau hors site (nécessitant l'utilisation d'un pare-feu personnel)
* les contrôles d'accès
* le cryptage du support de stockage
* la protection contre les logiciels malveillants
* la désactivation, suppression ou verrouillage à distance
* les sauvegardes
* l’utilisation de services Web et d'applications Web
* l’analyse du comportement de l'utilisateur final, cf. la procédure Activités de surveillance
* l'utilisation de dispositifs amovibles, y compris les supports de mémoire amovibles, et la possibilité de désactiver les ports physiques (ports USB)
* l'utilisation de capacités de partitionnement, si elles sont prises en charge par le terminal utilisateur (séparer en toute sécurité l’information de l'organisation des autres informations)

Il convient de déterminer si certaines informations sont si sensibles qu'elles ne sont accessibles que via les terminaux utilisateur, mais ne sont pas stockées sur ces terminaux. Dans de tels cas, des protections techniques supplémentaires peuvent être requises.

Exemples de protection :

* le téléchargement de fichiers pour le travail hors ligne est désactivé
* le stockage local tel que la carte SD est désactivé

Dans la mesure du possible, les recommandations relatives à cette mesure sont appliquées selon la gestion de la configuration, cf. le Registre de la configuration ou des outils automatisés.

**5.2 Responsabilité d’utilisateur**

Chaque utilisateur est informé des exigences de sécurité et des procédures de protection des terminaux, ainsi que de sa responsabilité dans l’application ces mesures de sécurité. Chaque utilisateur est avisé de :

* se désinscrire des sessions actives et mettre fin aux services lorsqu'ils ne sont plus nécessaires
* protéger les terminaux utilisateur contre toute utilisation non autorisée avec un contrôle physique (verrou à clé) et un contrôle logique (accès par mot de passe) lorsqu'ils ne sont pas utilisés, cf. Sécurité des appareils mobiles
* ne pas laisser les appareils contenant des informations commerciales importantes, sensibles ou critiques sans surveillance
* utiliser les appareils avec un soin particulier dans les lieux publics, les bureaux ouverts, les lieux de réunion et autres zones non protégées (éviter de lire des informations confidentielles en public)
* protéger physiquement les terminaux utilisateur contre le vol

Le document Sécurité des appareils mobiles prend en compte les exigences légales, statutaires, réglementaires, contractuelles (y compris les assurances) et autres concernant les cas de vol ou de perte des terminaux utilisateur.

**5.3 Utilisation d’appareils personnels**

Lorsque l'organisation autorise l'utilisation d'appareils personnels en plus des conseils donnés dans cette mesure, les éléments suivants sont pris en compte :

* séparer l'utilisation personnelle et professionnelle des appareils, y compris l'utilisation d'un logiciel pour prendre en charge cette séparation et protéger les données professionnelles sur un appareil privé
* fournir un accès aux informations commerciales uniquement après que l’utilisateur a reconnu ses obligations (protection physique, mise à jour logicielle, etc.), renonce à la propriété des données commerciales, permet l'effacement à distance des données par l'organisation en cas de vol ou de perte de l'appareil ou lorsqu'il n'est plus autorisé à utiliser le service. La législation sur la protection des DCP est envisagée, cf. la procédure Protection de la vie privée
* la procédure Propriété intellectuelle est appliquée pour prévenir les litiges concernant les droits de propriété intellectuelle développés sur des équipements privés
* l'accès à un équipement privé (pour vérifier la sécurité de la machine ou lors d'une enquête) peut être empêché par la législation
* des accords de licence de logiciel qui sont tels que les organisations peuvent devenir responsables de l'octroi de licence pour le logiciel client sur les terminaux utilisateur appartenant à des particuliers ou à des utilisateurs externes

**5.4 Connexions sans fil**

Le document Connexion sans fil précise les conditions et restrictions applicables :

* la configuration des connexions sans fil sur les appareils (désactivation des protocoles vulnérables)
* utilisant des connexions sans fil ou filaires avec une bande passante appropriée (en lien avec les sauvegardes ou les mises à jour logicielles nécessaires)