Protection contre les logiciels malveillants

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique de protection contre les logiciels malveillants**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2016 |
| **Page** | **Changement** | **Date** |

**1. Objet**

La politique de protection contre les logiciels malveillants a pour objet de montrer les exigences à respecter pour garantir le fonctionnement correct et sécurisé de nos systèmes opérationnels.

**2. Finalité**

La politique de protection contre les logiciels malveillants a pour finalité de protéger l’information et les moyens de traitement de l’information de toute ingérence externe.

**3. Domaine d’application**

La politique de protection contre les logiciels malveillants s’applique à tous les départements et actifs numériques de notre organisation.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de politique de protection contre les logiciels malveillants. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Gestion des vulnérabilités

Traitement de l’information

Transfert d’information

Mesures cryptographiques.

Formation et sensibilisation

Installation de logiciels

Inventaires des actifs

Protection contre les menaces extérieures

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

A.8.7 Protection contre les programmes malveillants

Une protection contre les programmes malveillants doit être mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs.

**7. Politique de protection contre les logiciels malveillants**

La lutte contre les risques d'attaque par des codes malveillants (virus, chevaux de Troie, spyware, vers, etc.) inclut :

* l’interdiction d'utiliser des logiciels non préalablement autorisés
* les mesures de protection lors de la récupération de fichiers via des réseaux externes
* la revue des logiciels installés

Les actions à entreprendre pour protéger les actifs de l’organisation sont :

* prévenir
* détecter
* réagir

L’abonnement à un centre d'alerte nous permet d'être prévenu et d'anticiper certaines attaques massives pour lesquelles les antivirus ne sont pas encore à jour.

Les programmes de prévention sont régulièrement et automatiquement mis à jour :

* anti-virus
* pare-feu
* anti-spam
* anti-hameçonnage
* anti-rançon

Un attaquant (agresseur) peut être :

* un plaisantin – pour s’amuser
* un compétiteur – pour voler
* un voleur – pour vendre
* un vandale – pour détruire
* un espion – pour voler et rendre service

Les serveurs de notre système et tous les postes de travail intègrent des dispositifs de protection contre les codes malveillants afin d’empêcher l'exploitation des vulnérabilités techniques. Plus de détails dans la politique Gestion des vulnérabilités.

Une analyse complète des fichiers des postes de travail est régulièrement effectuée de façon automatique.

Une passerelle antivirale permet l’inspection du trafic Internet et de la messagerie.

L’utilisation correcte et acceptable des équipements de communication est appliquée dans notre organisation. Plus de détails dans la procédure Traitement de l’information.

La procédure Transfert d’information établit les moyens de protection contre l’interception, la reproduction, la modification et la destruction de l’information au cours d’un transfert.

Des techniques de cryptographie afin de protéger la confidentialité, l’intégrité et l’authenticité de l’information sont utilisées. Plus de détails dans la politique Mesures cryptographiques.

Le personnel est sensibilisé de ne pas tenir de conversation confidentielle dans des lieux publics et sur des réseaux de communication non sécurisés. Plus de détails dans la procédure Formation et sensibilisation.

Les applications et les systèmes sensibles disposent d'une fonction automatique de surveillance en cas d'accumulation d'événements anormaux (par exemple tentatives malveillantes infructueuses de connexion ou d'intrusion).

Seuls les logiciels installés par le RSI sont utilisés sur les ordinateurs et les réseaux internes. Plus de détails dans la procédure Installation de logiciels.

La liste des logiciels autorisés est tenue à jour dans le fichier Inventaires des actifs.

Quelques règles à suivre de Protection contre les menaces extérieures :

* n'ouvrez jamais de fichiers (ou de macros) attachés à un courriel provenant d'une personne inconnue, suspecte ou de source non fiable. Supprimez ces pièces jointes immédiatement, puis "doublez-les" en vidant votre dossier poubelle
* supprimez les spams et autres courriels indésirables sans les ouvrir ou transférer
* avant d'utiliser une clé USB d'une source inconnue, toujours la soumettre à une analyse antivirus
* sauvegardez régulièrement vos données critiques sur un support sûr
* vérifiez périodiquement les mises à jour de votre antivirus
* éviter de surfer sur les sites suspects
* vérifiez la cohérence entre l’expéditeur présumé et le contenu du message. En cas de doute, n’hésitez pas à contacter directement l’émetteur du courriel
* ne répondez jamais par courriel à une demande d’informations personnelles ou confidentielles (comme code confidentiel et numéro de carte bancaire)
* n’ouvrez pas et ne relayez pas de messages de types chaînes de lettre (appels à la solidarité, alertes virales, vous avez gagné un prix)
* désactivez l’ouverture automatique des documents téléchargés
* ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie personnelle
* n’hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.)