**Chaîne TIC**

**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**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de maintenir un niveau convenu de sécurité de l’information dans les relations avec les fournisseurs.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Chaîne TIC » s’applique à l’ensemble du personnel ayant accès à l’information et aux autres actifs de l’organisation.

**1.3 Glossaire**

TIC – technologies de l’information et de la communication

RSI – responsable sécurité de l’information

SI – sécurité de l’information

**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**

Gérer la chaîne TIC

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

A.5.21 Chaîne TIC

Des processus et procédures doivent être définis et appliqués pour gérer les risques de sécurité de l'information liés à la chaîne d'approvisionnement des produits et services TIC.

**5. Déroulement**

Le processus Gérer la chaîne TIC prend en compte de la sécurité de la chaîne d'approvisionnement des TIC en plus des exigences générales de sécurité de l'information des relations avec les fournisseurs :

* définir les exigences de sécurité de l'information à appliquer lors de l'acquisition de produits ou de services TIC (fournisseur fiable)
* exiger que les fournisseurs de services TIC retransmettent les exigences de sécurité de l'organisation tout au long de la chaîne d'approvisionnement quand ils sous-traitent certaines parties du service TIC fourni à l'organisation
* exiger que les fournisseurs de produits TIC retransmettent des pratiques de sécurité appropriées tout au long de la chaîne d'approvisionnement quand ces produits comprennent des composants achetés ou acquis auprès d'autres fournisseurs (des développeurs de logiciels sous-traités et des fournisseurs de composants matériels)
* demander aux fournisseurs de produits TIC de décrire les composants logiciels utilisés dans les produits
* demander aux fournisseurs de produits TIC de fournir des informations décrivant les fonctions de sécurité mises en œuvre de leur produit et la configuration requise pour son fonctionnement sécurisé
* mettre en œuvre un processus de surveillance et des méthodes acceptables pour valider que les produits et services TIC fournis respectent les exigences de sécurité énoncées (tests d'intrusion, validation d'attestations tierces)
* mettre en place un processus d'identification et de documentation des composants de produits ou de services qui sont essentiels au maintien de la fonctionnalité et nécessitent une attention, un examen et un suivi accrus (le fournisseur sous-traite lui aussi)
* s’assurer que les composants critiques peuvent être retracés tout au long de la chaîne d'approvisionnement jusqu’à leur origine
* s’assurer que les produits TIC livrés fonctionnent comme prévu, sans fonctionnalités inattendues ou indésirables
* s'assurer que les composants des fournisseurs sont authentiques et correspondent à leurs spécifications (étiquettes anti-effraction, signatures numériques)
* prévenir et détecter la falsification pendant la conception, le développement, l'intégration, l'exploitation et la maintenance
* s’assurer que les produits TIC atteignent les niveaux de sécurité requis (certification formelle, système d'évaluation)
* définir les règles de partage d'information concernant la chaîne d'approvisionnement et tout problème potentiel entre l'organisation et les fournisseurs
* mettre en œuvre des processus spécifiques pour gérer le cycle de vie et la disponibilité des composants TIC et les risques de sécurité associés
* envisager un fournisseur alternatif et le transfert de logiciel et de compétence au fournisseur alternatif