Conformité aux règles et normes

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique conformité aux règles et normes**

Historique

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

**1. Objet**

La politique conformité aux règles et normes a pour objet d’identifier les obligations légales et réglementaires.

**2. Finalité**

La politique conformité aux règles et normes a pour finalité d'assurer que la sécurité de l'information est mise en œuvre et exploitée conformément à la politique de sécurité de l'information de l'organisation, aux politiques, règles et normes spécifiques.

**3. Domaine d’application**

La politique conformité s’applique à tous les départements et actifs 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 la politique conformité aux règles et normes. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Liste des exigences

Inventaire des actifs

Règles disciplinaires

Plan de classification

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

A.5.36 Conformité aux politiques, règles et normes de sécurité de l’information

La conformité à la politique de sécurité de l'information, aux politiques spécifiques, aux règles et aux normes de l'organisation doit être régulièrement vérifiée.

**7. Politique conformité aux règles et normes**

Le responsable sécurité de l’information (RSI) identifie les méthodes de revue du respect des exigences de sécurité de l’information définies dans la politique de sécurité de l’information, les politiques spécifique, les règles, les normes et autres réglementations applicables. Il a l’appui de la direction et des responsables des départements.

Le RSI identifie et tiens à jour l'ensemble des exigences réglementaires, contractuelles et légales applicables à notre organisation dans le fichier Liste des exigences.

L’inventaire des logiciels installés et les numéros de licence sur chaque équipement (serveurs, postes de travail, équipement réseau et de sécurité, …) est tenu à jour sur le fichier Inventaire des actifs.

L’audit de conformité des systèmes d’information est conduit régulièrement conformément au processus Auditer.

Le personnel est sensibilisé sur la protection des droits de propriété intellectuelle et les mesures disciplinaires qui peuvent s’appliquer, cf. le fichier Règles disciplinaires.

Des outils de mesure et de rapport automatiques sont envisagés pour obtenir une revue régulière et efficace.

Le RSI vérifie périodiquement que le nombre maximal d’utilisateurs autorisé par licence n’est pas dépassé.

La protection des enregistrements est réalisée conformément à leur classification telle que définie dans le Plan de classification.

Lorsqu’une non-conformité est identifiée à la suite de la revue, le RSI entreprend les activités suivantes :

* identifier les causes premières de la non-conformité
* évaluer la nécessité d'actions correctives pour assurer la conformité
* mettre en œuvre les actions correctives appropriées
* examiner les actions correctives prises pour vérifier leur efficacité et identifier toute omission ou faiblesse

Les actions correctives sont réalisées en temps opportun en fonction du risque. S'ils ne sont pas terminés lors du prochain examen prévu, les progrès sont au moins abordés lors de cet examen.

Le système de stockage des enregistrements garantit la durée de leur conservation selon la Liste des exigences.