Classification

**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 Classification de l’information**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure de classification de l’information a pour finalité d’assurer l'identification et la compréhension des besoins de protection de l’information en fonction de son importance pour l'organisation.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Classification de l’information » s’applique à l’information présente dans tous les produits et services proposés par notre organisation.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

RSI – responsable 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**

Classification de l’information

Plan de classification

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

A.5.12 Classification de l’information

L’information doit être classifiée conformément aux besoins de protection de l’information de l’organisation selon les exigences de confidentialité, d'intégrité et de disponibilité.

**5. Déroulement**

**5.1 Classification de l’information**

La protection de l’information et des actifs associés contre l'accès et la divulgation non autorisé sont critiques pour notre organisation.

La politique Classification de l’information est communiquée en interne et aux parties prenantes.

Les fournisseurs et sous-traitants sont informés de notre système de classification de l’information.

L’ensemble du personnel veille à ce que les actifs bénéficient d'un niveau de protection approprié en observant la classification de l’information :

* les responsables de département garantissent l'attribution de classification de l’information selon le système ci-dessous
* les informations externes (confiées à l’organisation) sont classifiées de la même manière
* la catégorie de l’information est intégrée à l'information elle-même, si possible
* tous les utilisateurs prennent en compte la catégorie de l’information lors de la protection des actifs

Le Plan de classification prend en compte les exigences de confidentialité, intégrité et disponibilité. Le plan est montré dans le tableau ci-dessous :

|  |  |  |
| --- | --- | --- |
| catégorie de l’information | description | exemple |
| publique | * pas de confidentialité * peut être non disponible momentanément * intégrité importante mais non vitale | * brochures * publicité * site web * démonstrations gratuites de logiciel |
| interne | * accès pour l’ensemble du personnel * peut avoir des conséquences financières * intégrité vitale | * mots de passe * procédures * instructions de travail * politiques |
| confidentielle | * propriété du client * ne peut être changée sans l’autorisation écrite du client * niveau très élevé d’intégrité, de confidentialité et de disponibilité | * informations du client * spécifications du client * informations des activités de l’organisation pour le client |
| secrète | * accès restreint et privilégié * peut avoir des conséquences financières très lourdes * niveau le plus élevé d’intégrité, de confidentialité et de disponibilité | * données personnelles * rapports financiers * accords confidentiels * plan stratégique de l’organisation |

Le plan de classification est utilisé partout dans l’organisation e dans tous les documents (processus, procédures, politiques, enregistrements).

Une information peut cesser d’être sensitive avec le temps.

Nous faisons attention à ne pas surclasser ou sous classer une information.