Classification de l’information

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique classification de l’information**

Historique

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

**1. Objet**

La politique classification de l’information a pour objet de décrire les méthodes utilisées pour classifier l’information conformément aux exigences de l’organisation et des parties intéressées.

**2. Finalité**

La politique 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.

**3. Domaine d’application**

La politique classification de l’information 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 classification de l’information. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Contrôle d'accès

Classification de l’information

Marquage

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

A.5.12 Politique de classification de l’information

Les informations doivent être classifiées conformément aux besoins de sécurité de l'information de l'organisme, sur la base des exigences de confidentialité, d'intégrité, de disponibilité et des exigences importantes des parties intéressées.

**7. Politique classification de l’information**

La politique classification de l’information est communiquée à toutes les parties intéressées concernées.

Le schéma de classification tient compte des exigences de confidentialité, d'intégrité et de disponibilité en vigueur dans l’organisation.

Les classifications et les mesures de protection associées tiennent compte :

* des besoins commerciaux en matière de partage ou de restriction de l’information
* de la protection de l'intégrité de l’information
* de l'assurance de la disponibilité
* des exigences légales concernant la confidentialité, l'intégrité et la disponibilité de l’information

Les actifs autres que l’information peuvent également être classés conformément à la classification de l’information, qui sont stockées dans, traitées par ou protégées par l'actif.

Les propriétaires de l’information sont responsables de leur classification.

Le système de classification inclut les conventions de classification et les critères de révision de la classification au fil du temps. Les résultats de la classification sont mis à jour en fonction des changements de valeur, de sensibilité et de criticité de l’information tout au long de son cycle de vie.

Le schéma de la classification est aligné sur la politique Contrôle d'accès et répond aux besoins commerciaux spécifiques de l'organisation.

La classification peut être déterminée par le niveau d'impact que la perte de l'information aurait pour l'organisation. Chaque niveau défini dans le schéma reçoit un nom qui a du sens dans le contexte de l'application du schéma de classification (publique, interne, confidentielle et secrète).

Le schéma est cohérent partout dans l'organisation et inclus dans les procédures afin que chacun classe l’information et les autres actifs associés applicables de la même manière. De cette manière, tout le monde a une compréhension commune des exigences de protection et applique une protection appropriée selon les procédures Classification de l’information et Marquage.

Le schéma de classification utilisé dans l'organisation peut être différent des schémas utilisés par d'autres organisations, même si les noms des niveaux sont similaires. De plus, l’information circulant entre les organisations peut varier en classification en fonction du contexte dans chaque organisation, même si leurs schémas de classification sont identiques. Par conséquent, les accords avec d'autres organisations qui incluent le partage d'information incluent des procédures pour identifier la classification de l’information et pour interpréter les niveaux de classification d'autres organisations. La correspondance entre différents schémas peut être déterminée en recherchant l'équivalence dans les modes de manipulation et de protection associés.

La classification fournit aux personnes qui traitent l’information une indication claire de gestion et de protection. La création de groupes d'informations ayant des besoins de protection similaires et la spécification de procédures de sécurité des informations qui s'appliquent à toutes les informations de chaque groupe facilitent cette tâche. Cette approche réduit la nécessité d'une évaluation des risques au cas par cas et d'une conception personnalisée des mesures.

Une information peut cesser d'être sensible ou critique après un certain temps.

Lorsque l'information a été rendue publique, elle n'a plus d'exigences de confidentialité mais peut encore exiger la protection de ses propriétés d'intégrité et de disponibilité.

Une sur-classification peut conduire à la mise en œuvre de mesures inutiles entraînant des dépenses supplémentaires ou, au contraire, une sous-classification peut conduire à des mesures insuffisantes pour protéger l’information.

Le schéma de classification de la confidentialité de l’information peut être basé sur les quatre niveaux suivants :

* la divulgation ne cause aucun dommage
* la divulgation cause des dommages mineurs à la réputation ou un impact opérationnel mineur
* la divulgation a un impact significatif à court terme sur les opérations ou les objectifs commerciaux
* la divulgation a un impact sérieux sur les objectifs commerciaux à long terme ou met la survie de l'organisation en danger