Restriction d’accès

**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 d’assurer uniquement l'accès autorisé et empêcher l'accès non autorisé à l’information et aux autres actifs associés.

**1.2 Domaine d'application**

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

**1.3 Glossaire**

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**

Contrôle d’accès

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

A.8.3 Restriction d’accès à l’information

L'accès à l’information et aux autres actifs doit être restreint selon la politique du contrôle d'accès.

**5. Déroulement**

L'accès à l'information et aux autres actifs associés est limité conformément à la politique Contrôle d’accès.

Pour les restrictions d’accès les éléments suivants sont pris en compte :

* ne pas autoriser l'accès aux informations sensibles par des identités d'utilisateurs inconnues ou de manière anonyme
* l'accès public ou anonyme n’est accordé qu'aux emplacements de stockage qui ne contiennent aucune information sensible
* des mécanismes de configuration sont appliqués pour contrôler l'accès à l’information dans les systèmes, les applications et les services
* contrôler quelles données peuvent être consultées par un utilisateur particulier
* contrôler quelles identités (ou quel groupe d'identités) ont quel accès, y compris la lecture, l'écriture, la suppression et l'exécution
* l'accès physique ou logique est contrôlé et isolé pour les applications, les données d'application et les systèmes sensibles

Les techniques de gestion dynamique des accès pour protéger les informations sensibles sont pris en compte lorsque l'organisation :

* nécessite un contrôle minutieux sur qui peut accéder à ces informations pendant quelle période et de quelle manière
* souhaite partager ces informations avec des personnes extérieures à l'organisation et garder le contrôle sur qui peut y accéder
* souhaite gérer dynamiquement, en temps réel, l'utilisation et la distribution de ces informations
* souhaite protéger ces informations contre les modifications, copies et distributions non autorisées (y compris l'impression)
* veut surveiller l'utilisation des informations
* souhaite enregistrer tout changement apporté à ces informations au cas où une enquête future serait nécessaire

Les techniques de gestion dynamique des accès protègent les informations tout au long de leur cycle de vie (la création, le traitement, le stockage, la transmission et l'élimination) et incluent l’établissement :

* des règles de gestion de l'accès dynamique basées sur des cas d'utilisation spécifiques en tenant compte :
  + des autorisations d'accès accordées en fonction de l'identité, de l'appareil, de l'emplacement ou de l'application
  + du schéma de classification afin de déterminer quelles informations doivent être protégées avec des techniques de gestion d'accès dynamique
* des processus opérationnels, de surveillance et de rapport et le soutien de l'infrastructure technique

Les systèmes de gestion d'accès dynamique protègent l’information en :

* exigeant une authentification, des informations d'identification appropriées ou un certificat pour accéder à l’information
* limitant l'accès (dans le temps)
* utilisant le cryptage pour protéger l’information
* définissant les autorisations d'impression de l’information
* enregistrant qui accède à l'information et comment l'information est utilisée
* déclenchant des alertes si des tentatives d'utilisation abusive de l’information sont détectées

Les techniques de gestion dynamique des accès et d'autres technologies de protection dynamique des informations peuvent être appliquées aux documents, courriels et autres fichiers contenant des informations pour limiter qui peut accéder au contenu et de quelle manière.

Les techniques de gestion d'accès dynamique ne remplacent pas la gestion d'accès classique, mais peuvent ajouter des facteurs pour la conditionnalité, l'évaluation en temps réel et la réduction des données juste à temps qui peuvent être utiles pour les informations les plus sensibles. C’est un moyen de contrôler l'accès en dehors de l'environnement de l'organisation.

La réponse aux incidents peut être prise en charge par des techniques de gestion d'accès dynamique, car les autorisations peuvent être modifiées ou révoquées à tout moment.