Gestion des identités

**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 Gestion des identités**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de permettre l'identification unique des individus et des systèmes accédant à l’information de l'organisation et aux autres actifs associés et de permettre une attribution appropriée des droits d'accès.

**1.2 Domaine d'application**

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

**1.3 Glossaire**

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

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**

Enregistrement et désinscription

Relations avec les fournisseurs

Authentification

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

A.5.16 Gestion des identités

Le cycle de vie complet des identités doit être géré.

**5. Déroulement**

**5.1 Gestion des identités**

Dans le cadre de la gestion des identités quelques règles à respecter :

* une identité spécifique n'est liée qu'à une seule personne (pour pouvoir tenir la personne responsable des actes accomplis avec cette identité)
* des identités attribuées à plusieurs personnes (identités partagées) ne sont autorisées que lorsqu'elles sont nécessaires pour des raisons commerciales ou opérationnelles et sont soumises à une approbation et à une documentation spécifiques
* les identités attribuées à des entités non humaines sont soumises à une approbation distincte appropriée et à une surveillance continue indépendante
* les identités sont désactivées ou supprimées en temps opportun si elles ne sont plus nécessaires (pour les entités supprimées ou ne sont plus utilisées, ou si la personne a quitté l'organisation ou a changé de rôle) selon le document Enregistrement et désinscription
* dans un domaine spécifique, une seule identité est liée à une seule entité (pour éviter les identités en double)
* des enregistrements de tous les événements significatifs concernant l'utilisation et la gestion des identités des utilisateurs et des informations d'authentification sont conservés

La gestion des changements de l’information relative à l’identité des utilisateurs est surveillée par le responsable du personnel.

Lors de l'utilisation d'identités fournies ou émises par des tiers (des données de médias sociaux), l'organisation s'assure que les identités tierces fournissent le niveau de confiance requis et que tous les risques associés sont connus et suffisamment traités. Ces activités de vérification sont réalisées selon les procédures Relations avec les fournisseurs et Authentification.