Droits 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**

**5.1 Attribution et suppression**

**5.2 Révision**

**5.3 Changement de poste ou fin de contrat**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité :

* d'assurer que l'accès à l’information et aux autres actifs associés est défini et autorisé en fonction des besoins de l'organisation
* d’assurer 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 « Droits d’accès » 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**

Distribuer les accès

Gérer les actifs

Contrôle d’accès

Droits d’accès

Distribution des accès

Revue des droits d’accès

Séparation des environnements

Descriptions de fonction

Appliquer la discipline

Règles disciplinaires

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

A.5.18 Droits d’accès

Les droits d'accès à l’information et aux actifs doivent être pourvus, révisés, modifiés et supprimés conformément à la politique spécifique et aux règles d’accès.

A.5.15 Contrôle d’accès

Des règles visant à contrôler l'accès physique et logique à l’information et aux autres actifs associés doivent être définies et mises en œuvre, en fonction des exigences métier et de sécurité de l'information.

**5. Déroulement**

**5.1 Attribution et suppression**

Le processus Distribuer les accès pour l'attribution ou la suppression des droits d'accès physiques et numériques accordés à l'identité authentifiée d'une entité inclut :

* l’obtention de l'autorisation du propriétaire de l’information et des autres actifs associés pour son utilisation, cf. le processus Gérer les actifs
* les exigences internes et des politiques Contrôle d’accès et Droits d’accès
* la séparation des tâches, cf. la procédure Séparation des environnements
* la suppression des droits d'accès en temps opportun lorsque une personne n'a plus besoin d'accéder à l’information et aux autres actifs associés
* des droits d'accès temporaires pour une durée limitée et de les révoquer à la date d'expiration (pour le personnel temporaire)
* la vérification du niveau d'accès accordé selon la politique de contrôle d'accès et la séparation des tâches (Descriptions de fonction)
* l’assurance que les droits d'accès ne sont activés qu'après la réussite de l'autorisation (pour les fournisseurs)
* l’enregistrement central des droits d'accès accordés ou modifiés, cf. Distribution des accès
* la modification des droits d'accès suite à un changement de poste
* la suppression des droits d'accès, au moyen de la suppression, la révocation ou le remplacement des clés, de l’information d'authentification, des cartes d'identification ou des abonnements

Les politiques Contrôle d’accès et Droits d’accès prennent en compte les éléments suivants :

* déterminer quelles entités nécessitent quel type d'accès à l’information et aux autres actifs associés
* la sécurité des applications
* l'accès physique, soutenu par des contrôles d'entrée physique appropriés
* la diffusion et l'autorisation de l’information (le principe du besoin de connaître)
* les niveaux de sécurité de l’information et sa classification
* les restrictions à l'accès privilégié
* la séparation des tâches
* la législation, la réglementation et toute obligation contractuelle pertinentes concernant la limitation de l'accès aux données ou aux services
* la séparation des fonctions de contrôle d'accès :
  + demande d'accès
  + autorisation d'accès
  + administration des accès
* l’autorisation formelle des demandes d'accès
* la gestion des droits d'accès
* la journalisation des accès
* la cohérence entre les droits d'accès et la classification de l’information
* la cohérence entre les droits d'accès et les besoins et exigences de sécurité du périmètre physique
* tous les types de connexions disponibles dans les environnements distribués
* comment les éléments ou facteurs pertinents pour le contrôle d'accès dynamique peuvent influer
* deux des principes les plus fréquemment utilisés :
  + besoin de connaître (accès à l’information dont cette entité a besoin pour accomplir ses tâches)
  + besoin d'utiliser (accès à l'infrastructure des technologies de l'information qu'en cas de besoin clair)
* établir des règles fondées sur le principe du moindre privilège (« Tout est généralement interdit sauf autorisation expresse », plutôt que la règle plus faible, « Tout est généralement permis sauf interdiction expresse »
* les modifications des étiquettes d'information déclenchées automatiquement par les moyens de traitement de l'information et celles déclenchées à la discrétion d'un utilisateur
* les modifications des autorisations des utilisateurs initiées automatiquement par le système d'information et celles initiées par un administrateur
* quand définir et réviser régulièrement l'approbation

**5.2 Révision**

Les révisions régulières des droits d'accès (cf. Revue des droits d’accès) prennent en compte :

* les droits d'accès des utilisateurs après tout changement (changement de poste, promotion, rétrogradation) ou fin de contrat
* les autorisations pour les droits d'accès privilégiés

**5.3 Changement de poste ou fin de contrat**

Les droits d'accès d'un utilisateur à l’information et aux autres actifs associés sont examinés et ajustés ou supprimés avant tout changement ou fin de contrat en fonction de l'évaluation de facteurs de risque tels que :

* si la résiliation ou le changement est initié par l'utilisateur ou par la direction et la raison de la résiliation
* les responsabilités actuelles de l'utilisateur
* la valeur des actifs actuellement accessibles

Les sanctions disciplinaire pour non-respect des exigences liées aux droits d’accès sont incluses dans le processus Appliquer la discipline et le document Règles disciplinaires.