Contrôle d’accès

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique contrôle d’accès**

Historique

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

**1. Objet**

La politique contrôle d’accès a pour objet de décrire les méthodes utilisées pour maîtriser l’accès à l’information et aux services d’information dans notre organisation.

**2. Finalité**

La politique contrôle d’accès a pour finalité de garantir l’accès autorisé aux utilisateurs et de protéger contre tout accès non autorisé.

**3. Domaine d’application**

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

**5. Documents**

Application

Accès visiteurs

Traitement de l’information

Classification de l’information

Marquage

Accès privilégiés

Propriété intellectuelle

Protection de la vie privée

Restrictions d’accès

Droits d’accès

Journalisation

Gestion des identités

Authentification

Accès au code source

Programmes utilitaires privilégiés

Engagement d’utilisateur

Revue des droits d’accès

Mots de passe

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

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 appliquées, en fonction des exigences métier et de sécurité de l'information.

A.5.18 Droits d’accès

Les droits d'accès à l’information et aux autres actifs associés doivent être pourvus, revus, modifiés et supprimés conformément à la politique spécifique à la thématique du contrôle d'accès et aux règles de contrôle d'accès de l'organisation.

A.8.2 Droits d’accès privilégiés

L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.

**7. Politique contrôle d’accès**

La politique contrôle d’accès est établie par le RSI et prend en compte les exigences métier et les exigences de sécurité de l’information.

La politique contrôle d’accès est communiquée aux parties prenantes concernées.

La politique contrôle d’accès tient compte des éléments suivants :

* déterminer quelles entités nécessitent quel type d'accès à l’information et aux autres actifs associés
* la sécurité des applications, cf. le fichier Application
* l'accès physique et les restrictions appropriées, cf. le fichier Accès visiteurs
* la diffusion et l'autorisation de l’information et sa classification, cf. les procédures Traitement de l’information, Classification de l’information et Marquage
* les restrictions à l'accès privilégié, cf. le fichier Accès privilégiés
* la séparation des tâches
* la législation, la réglementation et toute obligation contractuelle pertinentes concernant la limitation de l'accès aux données ou aux services selon les procédures Propriété intellectuelle, Protection de la vie privée et Restrictions d’accès
* la séparation des fonctions de contrôle d'accès :
  + demande d'accès
  + autorisation d'accès
  + gestion d’accès
* l’autorisation formelle des demandes d'accès et la gestion des droits d'accès selon la procédure Droits d’accès. Pour simplifier la gestion du contrôle d'accès, des rôles spécifiques peuvent être attribués à des groupes d'entités
* la journalisation des accès selon la politique Journalisation

Les éléments suivants sont pris en compte lors de la définition et de la mise en œuvre des règles de contrôle d'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 afin que les entités n'aient accès qu'à l’information et autres actifs associés, y compris les réseaux et les services de réseau, qu'elles sont autorisées à utiliser
* comment les éléments ou facteurs pertinents pour le contrôle d'accès dynamique sont influents

Principes généraux que nous utilisons :

* besoin de connaître : une entité n'a accès qu'à l’information dont cette entité a besoin pour accomplir ses tâches (différentes tâches ou rôles signifient différentes informations de connaître et donc différents profils d'accès)
* besoin d'utilisation : une entité ne se voit attribuer l'accès à l'infrastructure des technologies de l'information qu'en cas de besoin clair

Les précautions que nous prenons en compte  lors de la spécification des règles de contrôle d'accès :

* 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 du marquage de l’information selon la procédure Marquage déclenchées automatiquement par les installations 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
* tout accès distant au système d’information est toujours validé par le RSI
* quand définir et passer en revue régulièrement l'autorisation

Les règles de contrôle d'accès sont basées sur les procédures documentées et les responsabilités définies (Gestion des identités, Authentification, Droits d’accès, Restrictions d’accès, Accès au code source, Programmes utilitaires privilégiés).

Il existe plusieurs façons de mettre en œuvre le contrôle d'accès :

* obligatoire
* discrétionnaire
* basé sur les rôles
* basé sur les attributs

Les exigences commerciales et les considérations de risque sont utilisées pour définir quelles règles de contrôle d'accès appliquer et quelle granularité exiger.

Les systèmes de contrôle d'accès comprennent à la fois les systèmes internes (mots de passe, cryptage, listes des accès) et externes (dispositifs de protection des ports, pare-feu).

Les écrans de bannière préventive contiennent des déclarations indiquant que l'utilisation non autorisée du système est interdite et que les contrevenants feront l'objet de poursuites pénales.

L’accès pour les informations en nuage (*cloud*) suit les mêmes restrictions que pour les autres systèmes d’information.

L’information classée publique est accessible sans restriction sur le site WEB.

Chaque utilisateur s’engage de garder confidentielles les informations secrètes d'authentification et signe son Engagement d’utilisateur. Cet engagement est inclut dans le contrat de travail.

Les informations secrètes d'authentification par défaut des fournisseurs des systèmes ou des logiciels sont modifiées dès leur l'installation par le RSI.

Tous les identifiants de connexion des utilisateurs actifs sont vérifiés périodiquement par le RSI et enregistrés dans le fichier Revue des droits d’accès.

L'identifiant de connexion est verrouillé après un maximum de trois tentatives de connexion infructueuses. La réinitialisation de l’accès est réalisée par le RSI.

**Mots de passe**

Le système d’authentification permet aux utilisateurs de sélectionner et de modifier leurs propres mots de passe pour accéder au système et au poste de travail. Une confirmation de chaque mot de passe est exigée pour éviter les erreurs de frappe. Tout mot de passe est secret. Les règles recommandées sont établies dans le fichier Mots de passe.

Quand une personne quitte l’organisation son identifiant est bloqué.

Les moyens de traitement de l’information manipulant des données sensibles sont spécialement protégés.

Les moyens de stockage sont sécurisés contre tout accès non autorisé.

Des mesures sont adoptées pour réduire au minimum les risques de menaces physiques et environnementales comme :

* le vol
* le vandalisme
* l’incendie
* les explosions
* les inondations d’eau
* les vibrations
* les rayonnements électromagnétiques

Le règlement intérieur rappelle qu’il est interdit de manger, boire et fumer à proximité des moyens de traitement de l’information.

La température et l’humidité dans les locaux avec des moyens de traitement de l’information sont surveillées.

Le bâtiment est équipé d’un paratonnerre et toutes les lignes électriques et de télécommunication entrantes sont équipées de parafoudres.