Authentification

**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 de l’information d’authentification**

**5.2 Responsabilités de l’utilisateur**

**5.3 Système de gestion des mots de passe**

**5.4 Authentification sécurisée**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité :

* d’assurer une authentification appropriée de l'entité et éviter les échecs des processus d'authentification
* d’assurer qu'un utilisateur ou une entité est authentifié de manière sécurisée, lorsque l'accès aux systèmes, applications et services est accordé

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Authentification » 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

CAPTCHA - *Completely Automated Public Turing test to tell Computers and Humans Apart -* Test de Turing public entièrement automatisé pour différencier les ordinateurs des humains

**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**

Gérer l’authentification

Gestion des identités

Engagement d’utilisateur

Termes et conditions d’embauche

Utilisation de la cryptographie

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

A.5.17 Authentification

L'attribution et la gestion de l’information d'authentification doit être maîtrisée par un processus de management incluant des recommandations au personnel pour son utilisation appropriée.

A.8.5 Authentification sécurisée

Des technologies et procédures d'authentification sécurisées doivent être mises en œuvre sur la base des restrictions d'accès aux informations et de la politique spécifique à la thématique du contrôle d'accès.

**5. Déroulement**

**5.1 Attribution de l’information d’authentification**

Le processus Gérer l’authentification garantit que :

* les mots de passe personnels ou les numéros d'identification personnels (PIN codes) sont générés automatiquement lors des processus d'inscription
* l’utilisateur modifie le mot de passe attribué dès sa première utilisation
* la vérification de l'identité d'un utilisateur est effectuée avant de fournir des informations d'authentification nouvelles, de remplacement ou temporaires
* la transmission des informations d'authentification est réalisée de manière sécurisée
* les utilisateurs accusent réception des informations d'authentification
* les informations d'authentification par défaut (prédéfinies ou fournies par les fournisseurs) sont modifiées immédiatement après l'installation du système ou du logiciel
* la conservation et la confidentialité des enregistrements des événements significatifs concernant l'attribution et la gestion des informations d'authentification
* que la méthode d'enregistrement est approuvée

**5.2 Responsabilités de l’utilisateur**

Toute personne ayant accès à ou utilisant des informations d'authentification s'assure que :

* il a signé son Engagement d’utilisateur sur la confidentialité des informations d’authentification (les informations d'authentification secrètes telles que les mots de passe restent confidentielles)
* les informations d'authentification affectées ou compromises sont modifiées immédiatement après notification ou toute autre indication d'une compromission
* les mêmes mots de passe ne sont pas utilisés dans des départements et des systèmes distincts
* l'obligation de suivre les règles de responsabilité de l’utilisateur est incluse dans les conditions d'emploi, cf. le document Termes et conditions d’embauche

**5.3 Système de gestion des mots de passe**

Lorsque des mots de passe sont utilisés comme informations d'authentification, le système de gestion des mots de passe :

* permet aux utilisateurs de sélectionner et de modifier leurs propres mots de passe et inclut la validation (pour éviter les erreurs de saisie)
* oblige les utilisateurs à changer leurs mots de passe :
  + lors de la première connexion
  + après un incident de sécurité
  + suite à un changement d'emploi
* empêche la réutilisation des mots de passe déjà utilisés
* empêche l'utilisation de mots de passe :
  + couramment utilisés
  + de noms d'utilisateur compromis
  + de combinaisons de mots de passe provenant de systèmes piratés
* n’affiche pas les mots de passe à l'écran lors de leur saisie
* enregistre et transmet les mots de passe sous une forme protégée
* le cryptage et le hachage du mot de passe sont effectués conformément aux techniques cryptographiques, cf. Utilisation de la cryptographie
* demande d’appliquer des mots de passe forts conformément aux recommandations de bonnes pratiques :
  + les mots de passe ne sont pas basés sur quelque chose que quelqu'un d'autre peut facilement deviner ou obtenir à l'aide d'informations personnelles (prénom, nom, numéro de téléphone, date de naissance)
  + les mots de passe ne sont pas basés sur des mots du dictionnaire ou des combinaisons de ceux-ci
  + les mots de passe sont faciles à retenir et incluent des caractères alphanumériques et spéciaux
  + les mots de passe ont une longueur minimale

D'autres types d'authentification peuvent être utilisés :

* clés cryptographiques
* jetons matériels (cartes à puce)
* données biométriques (scans d'iris ou des empreintes digitales)

**5.4 Authentification sécurisée**

Une technique d'authentification appropriée est choisie pour justifier l'identité revendiquée d'un utilisateur, d'un logiciel, de messages et d'autres entités.

La force de l'authentification est adaptée à la classification de l’information accédée. Lorsqu'une authentification et une vérification d'identité fortes sont requises, des méthodes d'authentification alternatives aux mots de passe, telles que des certificats numériques, des cartes à puce, des jetons ou des moyens biométriques, sont utilisées.

Les informations d'authentification sont accompagnées de facteurs d'authentification supplémentaires pour accéder aux systèmes d'information critiques (authentification multi facteur).

Les informations d'authentification biométrique sont invalidées si elles sont compromises. L'authentification biométrique peut être indisponible selon les conditions d'utilisation (humidité ou vieillissement). L'authentification biométrique est accompagnée d'au moins une technique d'authentification alternative.

Les procédures et technologies de connexion minimisent le risque d'accès non autorisé et tiennent compte des éléments suivants :

* ne pas afficher les informations sensibles du système ou de l'application tant que le processus de connexion n'a pas été terminé avec succès (éviter de fournir à un utilisateur non autorisé une assistance inutile)
* afficher un avis général avertissant que le système ou l'application ou le service ne doit être accessible qu'aux utilisateurs autorisés
* ne pas fournir de messages d'aide pendant la procédure de connexion qui aideraient un utilisateur non autorisé (si une condition d'erreur survient, le système n’indique pas quelle partie des données est correcte ou incorrecte)
* valider les informations de connexion uniquement à la fin de toutes les données d'entrée
* protéger contre les tentatives de connexion par force brute sur les noms d'utilisateur et les mots de passe (test CAPTCHA, exiger la réinitialisation du mot de passe après un nombre prédéfini de tentatives infructueuses, bloquer l'utilisateur après un nombre maximum d'erreurs)
* enregistrer les tentatives infructueuses et réussies
* déclencher un événement de sécurité si une violation potentielle ou réussie des contrôles de connexion est détectée (envoyer une alerte à l'utilisateur et aux administrateurs système lorsqu'un certain nombre de tentatives de mot de passe erronées a été atteint)
* afficher ou envoyer les informations suivantes sur un canal séparé à la fin d'une connexion réussie :
  + date et heure de la précédente connexion réussie
  + les détails de toute tentative de connexion infructueuse depuis la dernière connexion réussie
* ne pas afficher un mot de passe en texte clair lors de sa saisie ; dans certains cas, il peut être nécessaire de désactiver cette fonctionnalité
* ne pas transmettre les mots de passe en clair sur un réseau pour éviter d'être capturé par un programme « renifleur » du réseau
* mettre fin aux sessions inactives après une période d'inactivité définie
* restreindre les durées de connexion (sécurité supplémentaire pour les applications à haut risque)