COLLEGES ET INSTITUT TECHNIQUE SAINT-VINCENT

POLITIQUE EN MATIÈRE DE MOTS DE PASSE

Version:	1.2
Date de la version :	15 juillet 2025
Créé par :	Vincent Willems, Responsable IT
Approuvé par :	Giacomo Amenta, DPO
Confidentialité :	Restreint

Historique des modifications

Date	Version	Créé par	Description de la mise à jour
23.03.2023	1.0	CES Saint-Vincent	Version alpha
09.10.2024	1.1	CES Saint-Vincent	Mise à jour mineure (logo)
15.07.2025	1.2	CES Saint-Vincent	Version conformité NIS2 (transmission des identifiants). Renforcement de la sécurité pour les utilisateurs des niveaux 7 à 9

Table des matières

1. Objectifs, champ d'application et utilisateurs 3
2. Documents de référence 3
3. Obligations de l'utilisateur 3
4. Gestion des mots de passe des utilisateurs 4
5. Validité et gestion des documents 5

1. Objectif, champ d'application et utilisateurs

Le présent document a pour objet de prescrire des règles visant à garantir la sécurité de la gestion et de l'utilisation des mots de passe.

Ce document s'applique à l'ensemble du champ d'application du système de gestion de la sécurité de l'information (SGSI), c'est-à-dire à tous les lieux de travail et à tous les systèmes situés dans le champ d'application du SGSI.

Les utilisateurs de ce document sont tous les employés le CES Saint-Vincent.

2. Documents de référence

- ISO/IEC 27001 standard, clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- Politique de sécurité de l'information
- Déclaration d'acceptation des documents ISMS

3. Obligations de l'utilisateur

Les utilisateurs doivent appliquer de bonnes pratiques de sécurité lors de la sélection et de l'utilisation des mots de passe :

- les mots de passe ne doivent jamais être divulgués à d'autres personnes, y compris à la direction et aux administrateurs du système
- les mots de passe ne doivent pas être écrits, à moins qu'une méthode sûre n'ait été approuvée préalablement par le responsable informatique
- les mots de passe générés par les utilisateurs ne doivent pas être distribués par quelque moyen que ce soit (oral, écrit, électronique, etc.)
- les mots de passe doivent être changés s'il y a des indications que les mots de passe ou le système ont pu être compromis - dans ce cas, un incident de sécurité doit être signalé
- des mots de passe forts doivent être choisis, utilisant au moins douze caractères et une combinaison d'au moins deux des éléments suivants :
    - au moins un caractère numérique
    - au moins une majuscule et au moins une minuscule
    - au moins un caractère spécial
    - un mot de passe ne doit pas être un mot du dictionnaire, un mot dialectal ou un mot de jargon d'une langue quelconque, ni aucun de ces mots écrit à l'envers
    - les mots de passe ne doivent pas être basés sur des données personnelles (par exemple, date de naissance, adresse, nom d'un membre de la famille, etc.)
    - les trois derniers mots de passe ne doivent pas être réutilisés
- les mots de passe doivent être changés tous les 3 mois
- le mot de passe doit être modifié lors de la première connexion à un système

- les mots de passe ne doivent pas être stockés dans un système de connexion automatisé (par exemple, une macro ou le navigateur web)
- les mots de passe utilisés à des fins privées ne doivent pas être utilisés à des fins professionnelles.

4. Gestion des mots de passe des utilisateurs

Lors de l'attribution et de l'utilisation des mots de passe des utilisateurs, les règles suivantes doivent être respectées :

- en signant la déclaration d'acceptation des documents SMSI (définissant les actions techniques et organisationnelles pour atteindre l'objectif), les utilisateurs acceptent également l'obligation de préserver la confidentialité des mots de passe, comme le prescrit le présent document
- chaque utilisateur ne peut utiliser que son propre nom d'utilisateur, qui lui est attribué de manière unique
- chaque utilisateur doit avoir la possibilité de choisir son propre mot de passe, le cas échéant
- the temporary password used for first system log-on must be unique and strong, as prescribed above
- le mot de passe temporaire utilisé pour la première connexion au système doit être unique et fort, comme prescrit ci-dessus
- les mots de passe temporaires doivent être communiqués à l'utilisateur de manière sécurisée, et l'identité de l'utilisateur doit être vérifiée au préalable
- le système de gestion des mots de passe doit exiger de l'utilisateur qu'il modifie le mot de passe temporaire lors de la première connexion au système
- le système de gestion des mots de passe doit exiger des utilisateurs qu'ils modifient leurs mots de passe tous les trois mois
- si l'utilisateur demande un nouveau mot de passe, le système de gestion des mots de passe doit déterminer l'identité de l'utilisateur en envoyant un courrier électronique demandant à l'utilisateur d'effectuer les actions nécessaires
- l'utilisateur doit confirmer la réception du mot de passe en se connectant au système dans un certain délai
- le mot de passe ne doit pas être visible à l'écran pendant la connexion
- si un utilisateur entre un mot de passe incorrect trois fois de suite, le système doit bloquer le compte d'utilisateur en question
- les mots de passe créés par le fabricant du logiciel ou du matériel doivent être modifiés lors de l'installation initiale
- les fichiers contenant les mots de passe doivent être stockés séparément des données système de l'application.

5. Niveaux d'accès et mesures de sécurité complémentaires

Les niveaux d'accès aux applications, dossiers partagés et Drives sont définis comme suit :

- **Niveau 0 :** visiteurs (aucun privilège)
- **Niveau 1** : élèves et parents
- **Niveau 2 :** stagiaires, personnel externe
- **Niveau 3 :** membres du personnel enseignant, membres des équipes PMS
- **Niveau 4 :** éducatrices et éducateurs (internet / externat)
- **Niveau 5** : Gestionnaire Interne des Accès (GIA), représentants du PO
- **Niveau 6 :** personnel administratif, en ce inclus les secrétaires de direction
- **Niveau 7 :** préfets et membres des équipes de direction
- **Niveau 8 :** Référent-e-s numériques
- **Niveau 9 :** Responsable IT, CISO, membre de la direction/administrateur référent IT.

Les utilisateurs des **niveaux 3 à 9** doivent activer l'authentification à double facteur dès la création de leur compte. Les utilisateurs des **niveaux 7 à 9** sont en outre soumis à l'obligation de mettre à jour leur mot de passe au moins tous les 120 jours.

6. Validité du présent document

Ce document est d'application à partir du 23.03.2023.

Le propriétaire de ce document est le responsable du service informatique, qui doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an.

Lors de l'évaluation de l'efficacité et de l'adéquation de ce document, les critères suivants doivent être pris en compte :

- nombre d'incidents liés à l'utilisation abusive des mots de passe par des personnes non autorisées
- nombre d'incidents liés à un traitement inadéquat des mots de passe

Le Responsable du service informatique