

## **POLITIQUE DE MOTS DE PASSE**

DI-1365-AD

PSSI - MS - 108

*Documentation Utilisateur*

Dans le cadre de sa Politique de Sécurité du Système d'Informations (PSSI) l'INERIS met en œuvre une politique de gestion des mots de passe destinée à minimiser le risque d'accès non autorisés aux systèmes d'information de l'INERIS.

Les mots de passe doivent être conformes à des règles de complexité et renouvelés périodiquement.

La durée maximum de validité d'un mot de passe (smartphone ou ordinateur) est de 90 jours. Passé ce délai il doit être changé sans réutiliser un ancien mot de passe.

Pour les Smartphones le code d'accès est composé de 6 caractères numériques.

Pour les ordinateurs et accès aux applications le mot de passe est conforme aux règles de sécurité suivantes :

- ✓ Le mot de passe doit comporter 12 caractères minimum
- ✓ Il doit être constitué de 3 types de caractères différents (\*)
- ✓ Il doit être différent de vos 8 derniers mots de passe
- ✓ Il ne peut pas être changé plus d'une fois par jour
- ✓ Il ne peut pas contenir votre nom et prénom

(\*) Combiner 3 types de caractères à choisir parmi les 4 familles suivantes :

On utilise principalement 4 types de caractères, **votre mot de passe doit au minimum en compter 3** :

- **Minuscules** des langues européennes (a à z, ainsi que les diacritiques, les caractères grecs et cyrilliques)
- **MAJUSCULES** des langues européennes (A à Z, ainsi que les diacritiques, les caractères grecs et cyrilliques)
- **Chiffres** (de 0 à 9)
- **Caractères spéciaux** : ~ ! @ # \$ % ^ & \* \_ - + = ` | \ ( ) } { [ ] : ; " ' < > , . ?

Pour les postes de travail, une info bulle Windows vous prévient 7 jours avant la date d'expiration de votre mot de passe.

Ce document vous apporte quelques conseils pour vous aider à gérer cette nécessité de changement de mot de passe régulière.

## I. POURQUOI CHANGER DE MOT DE PASSE ?

La résistance d'un mot de passe au piratage est directement fonction du nombre et du type caractères dont il est constitué.

Le tableau ci-dessous illustre le temps nécessaire à un logiciel de piratage pour compromettre la sécurité d'un compte, en fonction de la nature du mot de passe :

Longueur du mot de passe	Chiffres uniquement	Lettres minuscules & majuscules	Chiffres, lettres minuscules & majuscules	Chiffres, lettres min & maj, symboles
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

En se référant à ce tableau, si votre mot de passe est par exemple « Paul3007 » (8 caractères avec minuscules + majuscules + chiffres), il suffira de 10 jours pour le forcer en 2021 et bien moins dans les années à venir.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) demande l'utilisation de mots de passe d'au moins 12 caractères et de types différents (majuscules, minuscules, chiffres, caractères spéciaux). Ainsi qu'une modification de celui-ci tous les 90 jours.

**Un mot de passe divulgué ou forcé compromet la confidentialité des données de l'INERIS et de vos données personnelles.**

## II. CONSEILS - 4 exemples pour choisir un bon mot de passe

Pour vous aider à choisir voici quelques conseils pratiques pour obtenir un mot de passe à la fois sécurisé et facile à retenir.

### 1. TRANSFORMATION DE PHRASE :

Basez-vous sur une phrase simple comme « J'ai acheté huit cd pour cent euros cet après-midi » deviendra : « **ght8CD%E7am** »

### 2. PREMIERES LETTRES D'UN PROVERBE :

Transformez un proverbe en vous servant des premières lettres de chaque mot. « Pierre qui roule n'amasse pas mousse » pourra donner : « **Pqrn'@pm** »

### 3. MEMOIRE TACTILE :

Peut-être retenez-vous plutôt les gestes mécaniques, dans cette logique, vous pourriez utiliser par exemple une date historique couplée à la position de certaines touches du clavier :

**Q1s9d4f5** (1945 et la suite de lettres **qsdf**) ou **A1z5e1r5** (1515 et la suite de lettres **azer**)

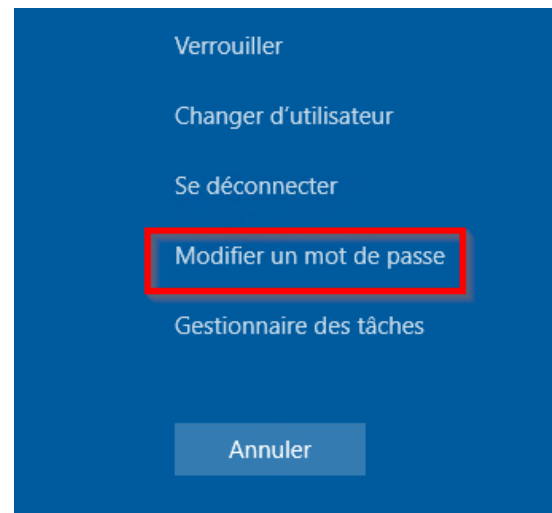
**Comment créer un mot de passe solide ? : N'utilisez pas un mot de passe, mais une phrase !**

### III. PROCEDURE DE CHANGEMENT DE MOT DE PASSE



Dans votre session Windows, appuyez **simultanément** sur les touches « **Ctrl + Alt + Suppr** » de votre clavier.

Cliquez sur :  
« **Modifier un mot de passe** »



- 1 - Tapez votre **mot de passe Windows actuel**
- 2 - Tapez votre **nouveau mot de passe**

Celui-ci doit respecter la politique en vigueur

- 3 - Retapez votre **nouveau mot de passe**
- 4 - **Validez**

## IV. EN CAS D'ERREUR

Si le nouveau mot de passe choisi **ne respecte pas la politique de sécurité de l'INERIS**, vous verrez apparaître le message suivant :



Cliquez sur **OK** et vérifiez que votre mot de passe respecte bien **tous** les critères définis :

- ✓ Le mot de passe doit comporter 12 caractères minimum
- ✓ Il doit être constitué de 3 types de caractères différents
- ✓ Il doit être différent de vos 8 derniers mots de passe
- ✓ Il ne peut pas être changé plus d'une fois par jour

Recommencez la procédure avec un nouveau mot de passe conforme aux règles de sécurité ci-dessus.

**Le centre de service DSI** reste à votre disposition pour toute question concernant le changement de votre mot de passe (Tel : **6666**).

## V. 8 TYPES DE MOTS DE PASSE A EVITER

1. Combinaisons de nombres ayant un rapport avec vous
2. Un dérivé de votre nom
3. Le nom d'un membre de votre famille
4. Le nom d'un de vos animaux domestiques
5. Un seul mot d'une langue donnée (facile à casser via des attaques de type « dictionnaire »)
6. Combinaisons simples du type 123456
7. Les termes tels que « motdepasse »

*Voici une liste de quelques-uns des mots de passe les plus utilisés et les moins efficaces au monde !*

« *motdepasse* »

« *123456* »

« *qwerty* »

« *111111* »

« *singe* »

« *password* »

« *abc123* »

« *iloveyou* »

« *adobe123* »

« *123123* »

« *sunshine* »

« *letmein* »

« *photoshop* »

*Ne pas noter son mot de passe sur un papier, car un mot de passe complexe (donc difficile à forcer) noté devient un mauvais mot de passe !*