Annexe au Règlement Intérieur de l'ESRG

Politique de gestion des mots de passe

Date de révision : 04.08.2025

La présente Politique s'applique à tous les « Utilisateurs » du système d'information de l'ESRG.

Est considéré comme « Utilisateur » toute personne ayant accès ou utilisant les ressources informatiques de L'ESRG et/ou ayant une habilitation lui conférant des droits et des accès particuliers dans le système d'information et de communication électronique.

Les Utilisateurs de l'organisation, dans l'exercice de leurs fonctions et de leurs obligations sont amenés à utiliser des mots de passe pour accéder aux systèmes et services de l'ESRG.

Dans un contexte global de multiplication des compromissions de bases de mots de passe, une politique de gestion de mots de passe a été mise en place pour garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles. Cette Politique définit les règles et les bonnes pratiques à suivre pour la création, l'utilisation et la protection des mots de passe.

Les Utilisateurs s'engagent à respecter les directives et bonnes pratiques énoncées dans cette politique.

1 – La complexité d'un mot de passe

Pour disposer d'un mot de passe suffisamment sécurisé, la CNIL recommande la création d'un mot de passe devant comporter au minimum :

- 12 caractères,
- Une combinaison de lettres majuscules et minuscules,
- Au moins un chiffre,
- Au moins un caractère spécial (exemple : @, #, $).

L'ESRG suggère aux utilisateurs de respecter cette recommandation et se l'applique pour la création d'un mot de passe communiqué à un Utilisateur de type « responsable bénévole de section » ou « encadrant sportif » par exemple.

2 – Le renouvellement régulier

Pour garantir une protection continue, les mots de passe :

- Gérés par l'ESRG seront renouvelés au plus tard au terme de chaque saison sportive ou en cours de saison si nécessité (exemple : changement dans la composition d'un Bureau de section)
- Gérés par un utilisateur : il est préconisé de changer régulièrement son mot de passe, exemple pour un adhérent lors de son renouvellement d'adhésion.

3 – La confidentialité

La confidentialité des mots de passe est impérative. Chaque Utilisateur est tenu de ne jamais divulguer ses mots de passe à l'extérieur de l'organisation, que ce soit par téléphone, par email ou sur des plateformes non sécurisées.

Pour des partages nécessaires les Utilisateurs devront passer par des gestionnaires de mots de passe sécurisés.

4 – L'utilisation de mots de passe différents pour chaque accès et l'activation de la double authentification

Afin de prévenir la compromission multiple, il est essentiel que les Utilisateurs mettent en place un mot de passe unique pour chaque compte.
De fait les mots de passe générés par l'ESRG sont uniques à un compte utilisateur ou pour l'accès à une information déterminée (exemple accès à un document de type « états de présences »).

De même, l'ESRG exige des Utilisateurs l'activation de la double authentification dès lors qu'elle est disponible. Cette mesure supplémentaire de sécurité, renforce l'authentification des Utilisateurs et réduit les risques d'accès non autorisés. Cette double authentification peut se faire par exemple via un identifiant nécessaire avant la saisie du mot de passe.