# Annexe 1 : charte informatique


Chapitre 1 : Sécurité de l'information 23

1.1/ Confidentialité et protection de l'information 23
1.2/ Droits d'accès au SI 23
1.3/ Gestion des moyens d'identification et d'authentification 23
1.4/ Accès à l'information 24
1.5/ Sauvegarde 24

Chapitre 2 : Sécurité du poste de travail 24

2.1/ Généralités 24
2.2/ Sécurité des accès distants et des portables 25
2.3/ Répertoires et fichiers personnels 25
2.4/ Stockage des données de travail 25
2.5/ Intervenants extérieurs 25

Chapitre 3 : Sécurité de la messagerie 25

3.1/ Règles de bon usage de la messagerie 25
3.2/ Contrôle de l'usage 26
3.3/ Utilisation de la messagerie à des fins privées 26

Chapitre 4 : Accès aux réseaux extérieurs 26

4.1/ Sécurisation des dispositifs de connexion et contrôle d'usage 26
4.2/ Accès à Internet 26
Règles d'usage de l'Internet 26
Utilisation d'Internet à des fins personnelles 27

Chapitre 5 : Cas particulier des responsables hiérarchiques 27

Chapitre 6 : Cas particulier des administrateurs informatiques 27

Chapitre 7 : Signalement des incidents 28

7.1/ Comment détecter un incident de sécurité ? 28
7.2/ Qui contacter ? 28
7.3/ Que faire ? 28

Chapitre 8 : Respect de la législation 29

8.1/ Législation concernant la protection de la propriété intellectuelle 29

Le Système d'Information (SI) comprend l'ensemble des ressources informatiques, matériels (micro-ordinateurs, serveurs, téléphonie, assistants personnels, télécopieurs, photocopieurs…), logiciels, applications et données accessibles à partir du poste de travail de l'utilisateur, soit directement, soit par les réseaux internes ou externes (RIE, Internet, partenaires, …).
Le SI est protégé par de multiples dispositifs (antivirus, anti spam, pare-feu, identification et authentification par mot de passe, droits d'accès aux ressources informatiques, procédures, etc.). Toutefois, ces dispositifs n'assurent pas une protection totale, et le facteur humain est un élément essentiel de la sécurité du SI.

Sont désignés sous le terme d'utilisateur toute personne ayant accès au SI :

- les agents du CREPS Provence-Alpes-Côte d'Azur, qu'ils soient dans les locaux de l'établissement ou en connexion distante ;
- les sportives et sportifs inscrits dans un pôle ;
- les stagiaires inscrits dans une formation professionnelle ;
- les tiers intervenants : prestataires, sous-traitants, ...

Le CREPS Provence-Alpes-Côte d'Azur dispose de deux réseaux informatiques distincts :

- un réseau privé dont l'interconnexion au réseau interministériel de l'État (RIE) se fait à l'aide du VPN CARINAE. Ce réseau est exclusivement réservé aux agents du CREPS Provence-Alpes-Côte d'Azur. Il donne accès de façon sécurisée aux ressources partagées (serveurs de fichiers, copieurs, autre) ;
- un réseau public et pédagogique, dédié principalement aux usagers, aussi appelé RPP.

Cette charte inscrite en annexe du règlement intérieur du CREPS Provence-Alpes-Côte d'Azur a pour objectif de préciser les règles et précautions que tout utilisateur du SI se doit de respecter.

Deux principes ont guidé la rédaction de cette charte :

- d'une part, l'utilisation et le bon usage du système d'information à des fins professionnelles ;
- d'autre part, la responsabilité de l'utilisateur par rapport à l'usage qu'il en fait, au regard du patrimoine collectif.

L'utilisateur est invité, par sa vigilance et les bonnes pratiques qu'il met en œuvre, à participer à la protection, au bon fonctionnement et à la construction de la confiance dans notre système d'information. Cette charte ne prétend pas à l'exhaustivité et n'est pas le mode d'emploi ou un référentiel technique de tous les éléments du SI. Les informations plus approfondies peuvent être trouvées dans des documents spécifiques à chaque élément du SI.

Le service informatique et réseaux est l'interlocuteur de l'utilisateur pour lui apporter appui et conseil en matière d'utilisation des systèmes d'information.

Le responsable des systèmes d'information et de communication (RSI) est le référent pour ce qui a trait au management de la sécurité des systèmes d'information.

## 1. Sécurité de l'information

### 1.1/ Confidentialité et protection de l'information

L'utilisateur doit adopter un niveau de protection en rapport avec la sensibilité de l'information (information non protégée, information en diffusion restreinte ou information confidentielle) et selon ses conditions de travail : dans son bureau, sur son poste de travail, hors de l'établissement avec des accès distants ou nomades.

### 1.2/ Droits d'accès au SI

L'accès au SI par l'utilisateur nécessite une identification et une authentification, c'est-à-dire un identifiant (nom de login) associé à un authentifiant (mot de passe).

### 1.3/ Gestion des moyens d'identification et d'authentification

L'utilisateur est responsable de l'utilisation du SI réalisée avec ses droits d'accès.
A ce titre, il doit assurer la protection des moyens d'authentification qui lui sont affectés : compte, mots de passe, certificats sur carte à puce, dispositif d'authentification forte type « clef USB ».
Le choix des mots de passe mérite une attention particulière. L'utilisateur doit respecter les prescriptions suivantes :

- il choisit des mots de passe sûrs : 8 caractères minimum, dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial ( !-{[|@...) ;
- lorsque le changement n'est pas imposé par le

système lui-même, l'utilisateur change ses mots de passe régulièrement, et au minimum tous les 90 jours ;
- il les garde secrets et s'oblige à les mémoriser, il s'interdit de noter ses mots de passe sur papier ou dans un fichier non protégé ou sur un fichier numérique de type texte.

Ces précautions s'appliquent à tous les comptes : réseau, messagerie, applications.

D'autre part, l'utilisateur ne doit jamais :
- communiquer ses mots de passe à un tiers, y compris à son responsable hiérarchique, ses collègues et à son correspondant informatique ;
- demander les mots de passe à un tiers, y compris à ses collaborateurs.

### 1.4/ Accès à l'information

L'utilisateur :
- assure la protection de ses informations, qu'elles soient sous forme numérique ou sous forme papier, selon le devoir de réserve de tout agent au sein de la fonction publique ;
- veille à ne pas mettre à la disposition de personnes non autorisées un accès aux systèmes d'information et à ne pas utiliser ou essayer d'utiliser des droits d'accès autres que les siens, en particulier l'accès physique au bureau. Une vigilance particulière doit s'exercer dans les entités accueillant du public ou partageant leurs locaux avec d'autres organismes ;
- ne tente pas de lire, modifier, copier ou détruire des données ou documents autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose du droit correspondant : lecture, modification ou suppression ;
- utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles (ordinateur portable, périphériques USB, etc.).

L'utilisateur prend les mesures de précaution nécessaires lorsqu'il quitte son poste de travail :
- écran de veille déclenché après vingt minutes au maximum ou poste verrouillé de façon manuelle ;
- déconnexion systématique de l'application utilisée lors d'une absence prolongée (repas…) ;
- extinction systématique du poste de travail en fin de journée ;
- rangement sous clef des cartes à puce, calculette, clé USB…
- fermeture des bureaux.

L'utilisateur garantit de plus à tout moment l'accès à ses données professionnelles, en cas d'empêchement ou de départ, en privilégiant systématiquement le stockage des fichiers d'intérêt général sur des répertoires partagés en réseau.

### 1.5/ Sauvegarde

Il est fortement recommandé de stocker ses fichiers sur les disques réseau mis à sa disposition. La sauvegarde est automatique et quotidienne sur les disques réseau. Aucune sauvegarde n'est assurée sur le poste de travail.
Chaque agent dispose d'un espace réseau privatif sur le serveur dans lequel. Il peut y stocker uniquement ses données de travail sensibles qu'il estime ne pas pouvoir partager avec autrui. Cet espace est sauvegardé dans les mêmes conditions que les espaces réseaux collaboratifs.
Les fichiers obsolètes doivent être détruits régulièrement. Il est interdit de stocker des fichiers personnels (vidéo, mp3, etc.) sur les espaces partagés.

## 2. Sécurité du poste de travail

### 2.1/ Généralités

Le CREPS Provence-Alpes-Côte d'Azur conçoit et configure un poste de travail répondant à un niveau de sécurité adapté aux besoins. Il veille notamment à ce que les logiciels installés sur l'ordinateur soient compatibles avec les autres éléments du système et les licences appropriées soient souscrites auprès des éditeurs de logiciels.
Seuls les équipements mis à disposition par le CREPS Provence-Alpes-Côte d'Azur (postes de travail fixe ou portables, périphériques USB, disque dur…) peuvent être connectés, de façon directe ou indirecte, au réseau professionnel.

L'utilisateur :
- ne doit jamais modifier lui-même la configuration de son poste de travail et de ses autres équipements. Ceci ne peut être réalisé que par le service informatique ;
- ne doit réaliser aucune copie de logiciels ;
- ne doit pas désactiver le logiciel anti-virus de son poste de travail ;

- ne doit pas faire obstacle aux mises à jour régulières (correctifs de sécurité et autres).
- s'interdit d'installer de nouveaux logiciels (en particulier, les logiciels de jeux et « barres d'outils » dans les navigateurs), en provenance d'Internet, de clés USB ou de cédéroms récupérés dans les revues informatiques. Toute installation de cette nature est absolument interdite ;
- prendra des précautions particulières avec les périphériques USB (clé, disque, lecteur mp3, appareil photo…) :
  - au niveau du poste de travail, il convient de désactiver la fonction « d'exécution automatique » pour ces périphériques ;
  - ne pas connecter des périphériques USB de provenance inconnue ;
  - ne pas prêter ou abandonner ses propres périphériques, sans les avoir nettoyés et formatés : ils peuvent contenir des données sensibles.

L'utilisateur est responsable de la protection des équipements mis à sa disposition. Il signale le plus rapidement possible à sa cellule informatique toute perte ou vol d'un équipement mis à sa disposition.

### 2.2/ Sécurité des accès distants et des portables

L'attention de l'utilisateur d'un micro-ordinateur portable et/ou de dispositifs d'accès distants est attirée sur les risques spécifiques inhérents à ce type d'équipement en matière de vol et de perte du matériel (y compris les périphériques amovibles) et de perte ou de divulgation des données.
Outre l'application scrupuleuse de toutes les recommandations de la présente charte, l'utilisateur bénéficiant d'un dispositif d'accès distant et/ou d'un portable :

- doit limiter au strict nécessaire la connexion de son ordinateur portable sur d'autres réseaux que ceux des services de l'État (notamment sur Internet, à domicile ou via des points d'accès Wifi), y compris lorsque l'agent est en télétravail ;
- doit protéger son ordinateur par un mot de passe au démarrage (mot de passe « BIOS ») ;
- doit veiller tout particulièrement à signaler dans les meilleurs délais toute perte ou vol de ces équipements nomades : portables, carte 3G, dispositif d'authentification forte.

### 2.3/ Répertoires et fichiers personnels

Les fichiers créés par l'utilisateur grâce aux outils informatiques mis à sa disposition sont présumés, sauf si l'utilisateur les identifie comme personnels, avoir un caractère professionnel, de sorte que le CREPS Provence-Alpes-Côte d'Azur peut y accéder hors de la présence de l'utilisateur.
Il appartient à l'utilisateur d'identifier les documents qui lui sont personnels, en les stockant par exemple dans un répertoire intitulé « privé » ou « personnel ».

### 2.4/ Stockage des données de travail

Les données produites dans le cadre des missions confiées à l'utilisateur par le CREPS Provence-Alpes-Côte d'Azur doivent être stockées sur les serveurs de l'établissement et dans un cadre plus général sur des supports accessibles par l'employeur (voir le point 9.5) et dont la confidentialité est assurée.
A ce titre, le stockage des données de travail, quelles qu'en soit la nature, dans des espaces de stockage en ligne (Dropbox, Google Drive, OneDrive, Memopal…) est strictement interdit.

### 2.5/ Intervenants extérieurs

La connexion temporaire d'ordinateurs d'intervenants extérieurs doit se faire exclusivement sur le Réseau WIFI « CREPSPACA » et avec les précautions d'usage : intervenants de confiance, ordinateurs à jour d'antivirus et de correctifs.

## 3. Sécurité de la messagerie

La messagerie est, avec le navigateur, l'un des moyens d'entrée possible des logiciels malveillants (virus, chevaux de Troie etc.) au sein d'une organisation.

### 3.1/ Règles de bon usage de la messagerie

L'utilisateur :

- est responsable des messages émis avec son adresse de messagerie ;
- veille à ce que le message émis ne porte pas atteinte à la personnalité, à la vie privée ou à l'activité professionnelle d'aucune personne, qu'elle soit agent du CREPS Provence-Alpes-Côte d'Azur ou extérieure ;
- ne stocke ni ne diffuse de messages ou de documents de contenu diffamatoire, discriminatoire (raciste, sexiste…), pornographique ou incitant à la violence ou la haine raciale, qui sont interdits et réprimés

par la loi ;

- s'abstient de faire suivre des messages « canulars » : fausses alertes aux virus ; fausses chaînes de solidarité ; fausses promesses etc. Dans le doute il sollicite le service informatique ;
- fait preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus, notamment de correspondants extérieurs. En effet, la falsification de l'identité de l'auteur d'un message est possible sur Internet ;
- ne doit pas utiliser à des fins professionnelles les services de sites web spécialisés dans la messagerie (messagerie webmail de type Gmail, Hotmail…), ces sites n'apportent aucune garantie de confidentialité ;
- veille à la protection des informations diffusées par messagerie. Une information confidentielle ne doit pas circuler par la messagerie standard ;
- s'abstient de toute tentative d'interception de messages dont il n'est pas destinataire ni directement, ni en copie ;
- La réémission (ou transfert) automatique vers une BAL (boîte à lettres) extérieure est strictement interdite sauf dans le cas de la mise à disposition par une autre administration d'une boite à lettre professionnelle : agents régionaux, agents disposant d'une boite « @ac-académie.fr » ou « @ eductaion.gouv.fr ».

### 3.2/ Contrôle de l'usage

Les messages avec des pièces jointes volumineuses (au-delà de 10Mo) sont susceptibles d'être supprimés au niveau des serveurs de messagerie de l'expéditeur ou du destinataire.

De même, les pièces jointes aux extensions dangereuses (*.exe, *.dll etc.) sont susceptibles d'être supprimées par les logiciels antivirus de l'expéditeur ou du destinataire.

Dans les deux cas, un message d'information concernant la suppression et la non-réémission est envoyé à l'émetteur.

### 3.3/ Utilisation de la messagerie à des fins privées

La messagerie est un outil de communication professionnelle.

L'usage à des fins personnelles, ponctuel et raisonnable, est admis, sauf pour les messages dont le but serait intéressé ou lucratif, voire contraire à la loi.

Il appartient à l'utilisateur d'identifier les messages qui sont personnels. A défaut d'une telle identification, les messages sont présumés être professionnels.

La nature personnelle d'un message peut par exemple être précisée de manière explicite dans l'objet du message (mention « personnel » ou « privé »).

## 4. Accès aux réseaux extérieurs

### 4.1/ Sécurisation des dispositifs de connexion et contrôle d'usage

Les connexions du réseau du CREPS aux réseaux extérieurs (ministères, autres partenaires) sont centralisées, et sécurisées à l'aide de dispositifs adaptés (pare-feu, antivirus…).

En outre, l'accès à Internet grand public est doté d'un mécanisme de filtrage d'adresses qui interdit les sites ou catégories de sites prohibés (sites à contenu raciste, pédophile,…). L'utilisateur doit, néanmoins, rester vigilant et s'interdire d'accéder à des sites illégaux.

Il est rigoureusement interdit d'installer sur les réseaux du CREPS un quelconque moyen d'accès à un autre réseau, et en particulier à Internet (ADSL, Wifi, etc.).

Il est rigoureusement interdit de contourner ou de tenter de contourner les dispositifs de protection et de contrôle (« proxy » pirate, « tunneling », prise de main à distance etc.).

### 4.2 Accès à Internet

Lorsqu'il est dans les locaux du CREPS, l'utilisateur ne doit accéder au réseau Internet qu'à partir de la connexion du réseau disponible et géré par le CREPS Provence-Alpes-Côte d'Azur.

En particulier, toute connexion (WIFI, courants porteurs (CPL), Bluetooth ou autre) non fournie par le CREPS est strictement interdite.

### Règles d'usage de l'Internet

L'utilisateur :

- ne doit jamais communiquer ses coordonnées, en particulier son adresse courriel professionnelle, sur des sites sans rapport avec son activité professionnelle. Celle-ci fait en effet clairement apparaître son appartenance au CREPS Provence-Alpes-Côte d'Azur et pourrait être utilisée à des fins illicites ;
- sauf accord écrit de sa hiérarchie, il s'interdit toute intervention sur Internet (blog par exemple) en faisant état de son appartenance à un service de l'Etat ;

- dans les réseaux "sociaux", l'utilisateur s'abstient de mentionner son appartenance et sa fonction au CREPS Provence-Alpes-Côte d'Azur hormis dans le cadre de la communication d'établissement telle que décrite par la mission partenariat communication ;
- ne doit pas faire usage de services et logiciels de messagerie instantanée et de téléphonie par Internet autres que ceux fournis par le CREPS ;
- réserve la consultation de contenu vidéo et audio en temps réel (streaming) à un usage professionnel.

### Utilisation d'Internet à des fins personnelles

L'utilisation d'Internet à des fins personnelles est tolérée dans le respect des règles mentionnées dans la présente charte.
Cette utilisation doit être raisonnable pour ne pas entraver l'utilisation professionnelle du système d'information et suivre les recommandations suivantes :

- l'utilisateur privilégie l'accès à Internet à des fins personnelles en dehors des plages à fort trafic sur le réseau, avant 8h00, de 12h30 à 13h30, et après 17h30 ;
- le téléchargement de fichiers volumineux doit être évité ;
- l'utilisateur s'engage à ne pas accéder aux sites illégaux ;
- l'utilisateur veille au respect du droit d'auteur en s'interdisant de télécharger des films, musiques, images et logiciels soumis à un droit de licence.

## 5. Cas particulier des responsables hiérarchiques

Les membres de l'équipe de direction, les responsables de département et les chefs de service du CREPS Provence-Alpes-Côte d'Azur sont soumis, en tant qu'utilisateurs des systèmes d'Information, aux règles décrites ci-avant.

Par ailleurs, du fait de leurs responsabilités hiérarchiques, ils sont également tenus de respecter les exigences suivantes :

- s'assurer que les droits d'accès accordés aux utilisateurs sous leur responsabilité correspondent à leurs missions et notamment que les droits d'accès d'utilisateurs quittant leur service sont bien supprimés ou désactivés ;
- saisir leur autorité hiérarchique et alerter les acteurs en charge de la Sécurité du SI de tout manquement grave résultant du non-respect des règles de sécurité, ou de tout incident significatif de sécurité survenu au CREPS Provence-Alpes-Côte d'Azur dans leur périmètre de responsabilité ;
- dans les cas d'infraction constatée ou suspectée à l'encontre des lois et règlements, procéder à la mise en place de mesures conservatoires préservant les preuves éventuelles (mise au coffre du serveur attaqué, du poste de travail de l'utilisateur en infraction, etc.) en l'attente du résultat de l'enquête administrative et/ou judiciaire ;
- alerter le service informatique du départ imminent d'un utilisateur sous sa responsabilité et contribuer à la récupération de la dotation informatique et téléphonique confié à dernier ;
- être le détenteur dépositaire de tous les dispositifs informatiques et téléphoniques mutualisés affectés au service (à l'exclusion des copieurs).

Plus généralement, ils facilitent l'instauration d'une « culture sécurité » :

- par leur exemplarité et une communication régulière sur les bonnes pratiques de protection de l'information et du système d'Information ;
- en se faisant le relais, sur leur périmètre de responsabilité, de la diffusion et de la mise en application du présent document ;
- par un soutien actif des services en charge de la mise en œuvre des règles de sécurité.

En aucun cas, un supérieur hiérarchique n'est autorisé à consulter le contenu de messages ou de documents à caractère privé sans accord explicite et écrit de l'intéressé, sauf cas particuliers prévus par la Loi.

## 6. Cas particulier des administrateurs informatiques

Tout agent ayant pour mission d'assurer des tâches d'administration des ressources informatiques du CREPS Provence-Alpes-Côte d'Azur est soumis à des règles spécifiques.
Les administrateurs bénéficient de privilèges élevés sur les ressources informatiques du CREPS. De part ces privilèges, ils sont tenus à un strict devoir de confidentialité et de discrétion. Ainsi :

- les informations confidentielles et/ou personnelles (traces informatiques, fichiers, contenus de bases de données, en-têtes de messages électroniques, etc.) auxquelles ils ont accès ne peuvent être utilisées qu'à des fins de diagnostic ou d'administration des systèmes, dans le strict respect de la règlementation en vigueur ;

- ils ne doivent pas accéder ou tenter d'accéder à des informations personnelles telles que le contenu de messages électroniques ne leur étant pas destinés ou des fichiers et répertoires manifestement et/ou explicitement personnels, sauf actions ponctuelles, en présence de l'utilisateur concerné et avec son autorisation expresse, ou sur demande du directeur dans les cas strictement prévus par la Loi ;
- ils n'autorisent personne à accéder à ces informations, sauf cas particuliers prévus par la Loi ou habilitations formelles et légitimes préalablement déclarées (délégation d'agenda, etc.) ;
- ils ne doivent pas chercher à obtenir des informations confidentielles en dehors des besoins liés à leurs missions ;
- ils ne doivent pas se connecter à une ressource sans l'autorisation expresse de la personne à qui elle est attribuée, notamment dans le cas d'une prise de main à distance sur un poste de travail, ou d'absence prolongée de la personne concernée.

Ils sont vigilants à ne jamais :

- abuser de leurs pouvoirs et de leurs privilèges sur les ressources informatiques. L'exercice malveillant des prérogatives d'un administrateur peut être constitutif d'une infraction pénale ;
- communiquer à des tiers non habilités des informations sur les systèmes qu'ils administrent.

Ils jouent de plus un rôle central dans la gestion des incidents de sécurité. Ainsi ils alertent la direction du CREPS (cf. 8.2) systématiquement pour l'informer de tout incident sécurité ou tout élément permettant de suspecter un incident de sécurité.

Il est de plus rappelé qu'ils sont chargés :

- de la gestion technique des droits des utilisateurs de leur périmètre, et veillent en particulier à la suppression des droits et comptes des utilisateurs ayant quitté le CREPS ;
- de veiller à bien supprimer tout fichier des disques durs et clés USB mis au rebut (par les outils de formatage et de suppression définitive de fichiers) ;
- de l'application dans les meilleurs délais des divers correctifs diffusés, notamment via le système Windows Update pour les systèmes Windows ;
- de l'impérative tenue à jour de l'antivirus des serveurs et ordinateurs personnels de leur parc.

## 7. Signalement des incidents

### 7.1/ Comment détecter un incident de sécurité ?

- En cas de comportement anormal (au sens disponibilité, intégrité, confidentialité) du poste de travail ou de l'application utilisée ou en constatant, par exemple, la suppression ou la modification de fichiers.
- Une machine opère des actions non commandées, le système s'arrête et redémarre tout seul.
- En cas de constatation de comportements ou évènements « suspects » : messagerie, vol ou perte de données, compromission de données personnelles ou confidentielles.
- Antivirus inhibé : le logiciel antivirus ne répond plus, ou est désactivé.
- Correspondants mécontents : l'utilisateur a reçu un courriel en provenance d'un ou plusieurs correspondants, qui prétendent que ses courriels sont infectés. Il faudra s'assurer de la malveillance et la traiter avec les moyens adéquats.

Un incident peut arriver à n'importe qui. Un agent n'a donc pas a priori à culpabiliser si son poste de travail est victime d'un incident de sécurité. Il est préférable au contraire qu'il signale librement son problème au service informatique. Tout retard dans le signalement peut avoir des conséquences graves sur l'ensemble du réseau et des postes connectés et peut croitre avec le temps.

### 7.2/ Qui contacter ?

L'utilisateur doit prévenir le plus rapidement possible le service informatique par mail à l'adresse service.informatique@creps-paca.sports.gouv.fr
En cas de problème de sécurité (uniquement), le RSI peut aussi être joint par téléphone au 04 42 93 80 65 et/ou par courriel à rsi@creps-paca.sports.gouv.fr

### 7.3/ Que faire ?

L'utilisateur, au plan technique, ne doit mener aucune action corrective ou d'investigation.
Le service informatique, en cas d'incident avéré, met tout en œuvre, en coopération avec les services du ministère, pour permettre une résolution rapide de l'incident :

- isolement des serveurs ou postes de travail concernés : il convient de déconnecter la machine suspecte (PC ou serveur) du réseau en débranchant le câble réseau ;

- il convient de pas éteindre ou redémarrer la machine pour permettre la recherche d'indices et de traces.

## 8. Respect de la législation

### 8.1/ Législation concernant la protection de la propriété intellectuelle

Le droit d'auteur relatif aux logiciels, fichiers, bases de données, images, enregistrements sonores ou vidéos est protégé (articles L122-4, L 335-2 et L 335-3 du code de la propriété intellectuelle).

### 8.2/ Législation concernant la protection de l'intégrité d'un système d'information

Tout système d'information est légalement protégé contre l'accès ou la tentative d'accès sans autorisation, contre son altération totale ou partielle et l'entrave de son fonctionnement (articles 323-1 à 323-7 du nouveau code pénal).

### 8.3/ Législation concernant le respect des libertés individuelles et la protection des données personnelles

Un agent du CREPS Provence-Alpes-Côte d'Azur peut être amené, dans le cadre de son activité professionnelle, à utiliser un fichier contenant des données personnelles qui permettent d'identifier directement ou indirectement une personne (liste nominatives, numéros de téléphone, âge, sexe…). Cette utilisation doit être effectuée dans le respect du Règlement Général sur la Protection des Données, entré en vigueur le 25 mai 2018 qui présente les règles en vigueur pour la création, l'utilisation et le partage de ces fichiers et de la loi Informatique et Libertés du 6 janvier 1978 modifiée le 20 juin 2018,

Ces dispositions s'appliquent aussi dans le cas où l'utilisateur crée pour la bonne exécution de sa mission un fichier simple (tableau EXCEL, document papier…) contenant des données personnelles. Il doit alors se rapprocher du service informatique et du délégué à la protection des données AVANT la constitution du fichier.

Les personnes concernées par le traitement disposent de droits d'opposition, d'accès, à la portabilité, à l'effacement, à la limitation et de rectification des données les concernant.

Le délégué à la protection des données est chargé de faire respecter cette mesure (voir l'annexe au règlement intérieur portant spécifiquement sur la protection des données).

### 8.4/ Législation concernant le secret de la correspondance

Le secret des correspondances émises par la voie des télécommunications est garanti (article 226-15 du nouveau code pénal). La loi incrimine «le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions».

### 8.5/ Obligation des agents de l'Etat

#### Obligation de discrétion

L'article 26 de la loi 83-634 du 13/07/1983 stipule que «les fonctionnaires sont tenus au secret professionnel dans le cadre de règles instituées dans le code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès à des documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent.»

Cette obligation s'impose à tous les personnels intervenants au CREPS Provence-Alpes-Côte d'Azur quel que soit leur statut : fonctionnaire, contractuel, vacataire, agent régional, …

#### Droits d'auteur

L'article L 131-3-1 du Code de la propriété intellectuelle stipule que les droits patrimoniaux des documents produits d'un agent de l'État, dans l'exercice de ses fonctions ou d'après les instructions de son employeur, sont cédés de plein droit à l'employeur pour ce qui est strictement nécessaire à l'accomplissement de missions de service public.

L'article L 121-7-1 du Code de la propriété intellectuelle stipule que le droit de divulgation reconnu à l'agent qui a créé le document, dans l'exercice de ses fonctions ou d'après les instructions reçues, s'exerce dans le respect des règles auxquelles il est soumis en sa qualité d'agent public et dans le respect de celles que régissent dans l'organisation la fonctionnement et l'activité de la personne publique qui l'emploi.

L'agent public ne peut donc :

- s'opposer à la modification d'un document décidée dans l'intérêt du service par l'autorité investie du pouvoir hiérarchique dès lors que cette modification ne porte pas atteinte à son honneur ou à sa réputation
- ni exercer son droit de retrait ou de repentir sauf accord préalable de l'autorité investie du pouvoir hiérarchique.

L'utilisateur ne peut donc soustraire l'accès à ses documents de travail à son employeur en les stockant sur des supports non approuvés par ce dernier.

### 8.6/ Traçabilité

Le CREPS Provence-Alpes-Côte d'Azur est tenu de mettre en place des systèmes de journalisation des accès Internet, de la messagerie et des données échangées.

Des outils de traçabilité sont mis en place sur tous les systèmes d'information conformément aux règlementations en vigueur.

## 9. Documents de référence

Loi n°78-17 du 6 janvier 1978 « informatique, fichiers et libertés »

Loi n°85-660 du 3 juillet 1985 sur la protection des logiciels

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique

Loi n°95-597 du 1er juillet 1992 « code de la propriété intellectuelle »

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet,

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales, version du 1er octobre 2015

# Annexe 2 :
# charte sur la protection des données individuelles


1/ Article 1 : Identité du responsable de Traitement 32

2/ Article 2 : Finalités de la collecte de données à caractère personnel 32

3/ Article 3 : Les données à caractère personnel collectées 32

4/ Article 4 : Fondements juridiques des Traitements de données 33

5/ Article 5 : Destinataires des données 33

6/ Article 6 : Durée de conservation des données 33

7/ Article 7 : Sécurité des données 33

8/ Article 8 : Les droits des personnes sur leurs données à caractère personnel 33

Article 8.1 : Droit à l'information et d'accès aux données personnelles 33
Article 8.2 : Droit de rectification 34
Article 8.3 : Droit à l'effacement 34
Article 8.4 : Droit d'opposition 34
Article 8.5 : Droit à la limitation 34
Article 8.6 : Droit à la portabilité 35
Article 8.7 : Droits relatifs à une prise de décision individuelle automatisée et au profilage 35

9/ Références et personnes à contacter 35

La présente Charte annexée au Règlement intérieur a pour objet de présenter les engagements du CREPS Provence-Alpes-Côte d'Azur envers les données à caractère personnel de ses usagers et de son personnel.
Elle témoigne de son attachement envers les Droits et Libertés fondamentales des personnes, notamment du droit au respect de leur vie privée consacré à l'article 12 de la Déclaration Universelle des Droits de l'Homme (DUDH) de 1948, l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen (DDHC) de 1789, l'article 9 du Code civil de 1803 et l'article 8 de la Convention européenne des Droits de l'Homme (CEDH) de 1959.
La protection des données à caractère personnel fait depuis l'objet d'une protection autonome notamment par la loi Informatique et Libertés du 6 janvier 1978 modifiée le 20 juin 2018, et par le Règlement général sur la protection des données (RGPD) adopté par le Parlement européen le 27 avril 2016.
Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

## Article 1 : Identité du responsable de Traitement

Etablissement siège et site d'Aix-en-Provence :
CREPS Provence-Alpes-Côte d'Azur, 62 Chemin du Viaduc, 13090 Aix-en-Provence
Site de Boulouris-Saint-Raphaël : 346 Boulevard des Mimosas, 83700 Saint-Raphaël
Site d'Antibes : 50 Avenue du 11 Novembre, 06600 Antibes
Responsable de Traitement : M. Jérôme ROUILLAUX, Directeur Général.

## Article 2 : Finalités de la collecte de données à caractère personnel

Le CREPS Provence-Alpes-Côte d'Azur est amené à traiter des données à caractère personnel, tant pour les agents quel que soit leur statut, que pour les sportives et sportifs inscrits en pôle, que pour les stagiaires de la formation professionnelle et pour les usagers. Les données collectées sont uniquement les données nécessaires à la réalisation des finalités des traitements mis en œuvres, détaillés dans le Registre des traitements de données à caractère personnel du CREPS Provence-Alpes-Côte d'Azur. Le CREPS Provence-Alpes-Côte d'Azur s'engage à ne pas collecter plus de données que nécessaire.
Les finalités du CREPS Provence-Alpes-Côte d'Azur sont définies dans un objectif d'accomplissement de ses missions envers ses usagers, et dans le respect des obligations légales et réglementaires envers son personnel.

## Article 3 : Les données à caractère personnel collectées

Le CREPS Provence-Alpes-Côte d'Azur peut être amené à constituer un ou plusieurs fichiers comprenant des données personnelles pour permettre aux usagers de bénéficier des services ou pour remplir ses obligations légales.
Ces données peuvent être collectées auprès de la personne directement, ou transmises par des tiers partenaires du CREPS Provence-Alpes-Côte d'Azur notamment dans des cas de transfert de dossier.
Les données collectées sont détaillées dans le registre des traitements de données à caractère personnel du CREPS Provence-Alpes-Côte d'Azur.
Les données collectées des usagers du CREPS Provence-Alpes-Côte d'Azur peuvent consister en :

- Données nominatives, de vie professionnelle (diplômes, parcours scolaire, indicateurs de performance…), de vie personnelle (situation maritale, identité des titulaires de la responsabilité parentale si usager mineur…), des données de santé, des données de connexion.

## Article 4 : Fondements juridiques des Traitements de données

Pour justifier ses Traitements de données à caractère personnel, le CREPS Provence-Alpes-Côte d'Azur pourra se fonder sur les conditions suivantes :

- Obtention du consentement de la personne concernée ;
- Traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie prenante ;
- Traitement nécessaire au respect d'une obligation légale à laquelle le CREPS Provence-Alpes-Côte d'Azur est soumis ;
- Traitement nécessaire aux fins des intérêts légitimes poursuivis par le CREPS Provence-Alpes-Côte d'Azur ou par un tiers, à moins que ne prévalent les intérêts ou Libertés et Droits fondamentaux de la personne concernée.

## Article 5 : Destinataires des données

Les données sont destinées au CREPS Provence-Alpes-Côte d'Azur pour l'exercice de ses finalités. Les données pourront être transmises en interne aux services concernés, en respectant leur intégrité et confidentialité selon leur nature.

En vertu de sa nature d'établissement public local de formation, placé sous la double tutelle du ministère de l'Education Nationale, de la Jeunesse et des Sports et de la région Provence-Alpes-Côte d'Azur, des données pourraient être transmises aux tutelles ainsi qu'à des collectivités territoriales locales, ainsi qu'à d'autres établissements publics (organismes de formation…), toujours dans l'intérêt et pour une meilleure administration des dossiers des usagers et du personnel, ainsi que pour répondre à des exigences légales.

Dans le cadre d'organisation d'évènements, le CREPS Provence-Alpes-Côte d'Azur pourrait être amené à transmettre des données à des partenaires extérieurs, avec le consentement des usagers (tournois, échanges…), potentiellement dans des pays tiers, internes ou externes à l'Union européenne. Ces transmissions seront strictement limitées à ce qui est nécessaire, et seront encadrées juridiquement selon l'adéquation de chaque pays tiers aux normes de protection des données à caractère personnel en vigueur au sein de l'Union européenne.

## Article 6 : Durée de conservation des données

Les données à caractère personnel des usagers et du personnel ne seront conservées que pour le temps nécessaire pour les finalités poursuivies ou selon l'observation d'obligations légales de conservation, telles que décrites dans le Registre des traitements de données à caractère personnel du CREPS Provence-Alpes-Côte d'Azur.

Une fois cette durée écoulée, les données seront détruites ou anonymisées à des fins de recherche ou de statistique.

## Article 7 : Sécurité des données

Le responsable de traitement protège les données à caractère personnel des usagers et du personnel en mettant en place toutes les mesures techniques et organisationnelles nécessaires et proportionnelles pour assurer leur intégrité et leur confidentialité.

Le responsable de traitement a détaillé son engagement en matière de sécurité dans la charte informatique présente en annexe du règlement intérieur.

Au-delà, il en va de la responsabilité de tous, usagers et membres du personnel, de respecter les données à caractère personnel d'autrui. La présence de mesures techniques et organisationnelles ne saurait pallier l'absence de discrétion de chacun en la matière.

## Article 8 : Les droits des personnes sur leurs données à caractère personnel

Conformément à la règlementation en vigueur, les personnes disposent des droits suivants :

### Article 8.1 : Droit à l'information et d'accès aux données personnelles

Toute personne peut demander au responsable de Traitement si des données à caractère personnel la concernant sont ou ne sont pas traitées. Si c'est le cas, la personne concernée peut obtenir une copie des données à caractère personnel faisant l'objet d'un traitement ainsi que les informations suivantes :

- Les finalités du traitement ;
- Les catégories de données à caractère personnel concernées ;

- Les destinataires ou catégories de destinataires des données ;
- Lorsque cela est possible, la durée de conservation des données envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;
- Le cas échéant, l'existence d'une prise de décision automatisée, y compris un profilage, et les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce Traitement pour la personne concernée.

### Article 8.2 : Droit de rectification

Toute personne dont les données à caractère personnel font l'objet d'un traitement dispose du droit d'obtenir la rectification de ces données les concernant si celles-ci seraient inexactes, et que ces données soient complétées si la finalité du traitement le requiert.

### Article 8.3 : Droit à l'effacement

Toute personne dont les données à caractère personnel font l'objet d'un traitement du CREPS Provence-Alpes-Côte d'Azur a le droit d'obtenir l'effacement desdites données dans les cas suivants :

- Lorsque les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- Lorsque la personne concernée retire son consentement sur lequel était fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement ;
- Dans l'hypothèse où le traitement est fondé sur l'intérêt légitime du responsable du traitement, lorsque la personne concernée s'est opposée au traitement et qu'il n'existe pas de motif légitime impérieux pour le traitement ;
- Lorsque la personne concernée s'est opposée à un traitement ayant pour finalité la prospection ou le profilage lié à une telle prospection ;
- Lorsque les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- Lorsque les données à caractère personnel doivent être effacées pour respecter une obligation qui est prévue par le droit de l'union ou par le droit français auquel le responsable du traitement est soumis.

Le CREPS Provence-Alpes-Côte d'Azur pourra toutefois refuser d'effacer les données dans les cas suivants :

- Pour respecter une obligation qui requiert le traitement prévue par le droit de l'union ou par le droit français ;
- Lorsque le traitement a pour unique objet des fins statistiques ;
- Lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

### Article 8.4 : Droit d'opposition

Toute personne dont les données à caractère personnel font l'objet d'un traitement dispose d'un droit d'opposition à ce traitement dans les conditions suivantes :

- Lorsque le traitement est fondé sur la satisfaction des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, pour des raisons tenant à sa situation particulière et si le responsable du traitement ne démontre pas qu'il existe des motifs légitimes et impérieux pour le traitement prévalant sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice ;
- Lorsque le traitement est mis en œuvre à des fins de prospection ou de profilage lié à une telle prospection ;
- Lorsque le traitement est mis en œuvre à des fins statistiques, pour des raisons tenant à sa situation particulière.

### Article 8.5 : Droit à la limitation

Toute personne dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable du traitement sa limitation. Les données seront alors gelées, dans les cas suivants :

- Lorsqu'elle conteste l'exactitude de ses données à caractère personnel, pendant une durée permettant au responsable du traitement de vérifier l'exactitude desdites données ;
- Lorsque le traitement n'est pas conforme à la règlementation mais que le titulaire des données ne souhaite pas les effacer ;
- Lorsque le responsable du traitement n'a plus

besoin des données à caractère personnel aux fins du traitement mais que celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- Lorsqu'elle s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

Lorsque le traitement a été limité, à l'exception de la conservation, les données ne peuvent être traitées que dans les cas suivants :
- Avec le consentement de la personne concernée ;
- Pour la constatation, l'exercice ou la défense de droits en justice ;
- Pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

Si la limitation devait ensuite être levée, le responsable du traitement en informera au préalable la personne concernée.

### Article 8.6 : Droit à la portabilité

Toute personne dont les données à caractère personnel font l'objet d'un traitement peut solliciter du responsable du traitement qu'il lui communique ces données ou les transmette à un autre responsable du traitement dans les cas suivants:
- Lorsque le traitement a été mis en place suite au consentement de la personne concernée ;
- Lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie prenante ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- Lorsque le traitement est effectué à l'aide de procédés automatisés.

### Article 8.7 : Droits relatifs à une prise de décision individuelle automatisée et au profilage

Toute personne peut demander que les décisions produisant un effet juridique ou affectant de manière significative les personnes, fondées sur un traitement automatisé concernant ou affectant de manière significative la personne et fondées sur ses données à caractère personnel, soient prises par des personnes physiques et non uniquement par des ordinateurs. Dans ce cas, la personne a également le droit d'exprimer son avis et de contester lesdites décisions ;

Toute personne peut contester les décisions produisant un effet juridique ou affectant de manière significative les personnes, fondées sur un traitement de profilage, reposant sur l'établissement d'un profil individualisé. La personne a également, en vertu de son droit d'accès, le droit de demander une explication du raisonnement permettant la qualification de la personne.

Toutefois, le CREPS Provence-Alpes-Côte d'Azur pourra opérer de tels traitements dans les cas suivants :
- Par l'obtention du consentement explicite des personnes concernées ;
- Les décisions prises sont nécessaires à la conclusion et à l'exécution d'un contrat ;
- Les décisions sont encadrées par des dispositions légales spécifiques.

En cas de décès et dès qu'il a été porté à la connaissance du CREPS Provence-Alpes-Côte d'Azur, le CREPS Provence-Alpes-Côte d'Azur s'engage à transmettre les données dans les meilleurs délais au tiers désigné, ou à défaut à les détruire ou à les anonymiser. Toutefois, le CREPS Provence-Alpes-Côte d'Azur pourra conserver une copie des données à caractère personnel si nécessaire à des fins probatoires ou pour répondre à une obligation légale.

## 9. Références et personnes à contacter

Pour en savoir plus sur vos droits, vous pouvez trouver davantage d'informations sur le site de la CNIL :

www.cnil.fr/fr/comprendre-vos-droits

www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles#mortnumerique

Pour exercer l'un de ces droits, la personne concernée peut adresser sa demande au Délégué à la Protection des données Personnelles (DPD), en utilisant l'une des coordonnées suivantes :
- Par courrier : CREPS Provence-Alpes-Côte d'Azur (siège) - Délégué à la Protection des données Personnelles (DPD), 62, chemin du Viaduc, 13090 Aix-en-Provence (Accompagné d'un justificatif d'identité (copie de pièce d'identité))
- Par courriel : dpd@creps-paca.sports.gouv.fr (Accompagné d'un justificatif d'identité (copie de

pièce d'identité) si le courriel utilisé est différent du courriel présent dans son dossier ou du courriel utilisé pour son inscription).

Le CREPS Provence-Alpes-Côte d'Azur traitera la demande dans un délai de un (1) mois. Toutefois, compte tenu de la complexité de la demande ou de la présence d'un grand nombre de demandes, le délai peut être porté à deux (2) mois.
En cas de refus de traiter la demande, le CREPS Provence-Alpes-Côte d'Azur délivrera une réponse motivée dans le délai imparti.

Enfin, les personnes concernées ont également la possibilité de déposer une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), www.cnil.fr/fr/plaintes.