AGENCE FRANÇAISE
DE LUTTE CONTRE LE DOPAGE

La Présidente

Décision n° 2026-4 du 12 mars 2026
relative aux conditions de travail, d'hygiène et de sécurité

La Présidente de l'Agence française de lutte contre le dopage

Vu le code général de la fonction publique, notamment son article L. 136-1,

Vu le règlement intérieur de l'Agence française de lutte contre le dopage, notamment son chapitre VI,

Sur la proposition du secrétaire général,

DÉCIDE :

Chapitre Ier
Hygiène et sécurité

Article 1er : Les locaux et installations de service doivent être aménagés et les équipements doivent être réalisés et maintenus de manière à garantir la sécurité des agents et des usagers. Les locaux doivent être tenus dans un état constant de propreté et présenter les conditions d'hygiène et de sécurité nécessaires à la santé des personnes.

Article 2 : Des dispositifs de premier secours (armoire à pharmacie, défibrillateur, etc.) sont installés dans les locaux. Une information sur les agents formés aux premiers secours est affichée dans les locaux.

Seules les personnes habilitées sont autorisées à manipuler les matériels de secours (extincteurs, etc.).

Article 3 : Un registre est ouvert auprès du service de l'administration générale et des systèmes d'information. Il contient les observations et suggestions des agents relatives à la prévention des risques professionnels et à l'amélioration des conditions de travail ainsi que les situations ayant conduit à un droit d'alerte ou un droit de retrait de la part d'un agent.

Ce registre est mis à la disposition de l'ensemble des agents. Il est consultable par les représentants du personnel.

Article 4 : Lorsqu'un agent porte à la connaissance de son supérieur hiérarchique ou du secrétaire général un danger grave et imminent pour sa santé et sa sécurité, ce dernier prend les mesures et donne les instructions nécessaires pour permettre aux agents d'arrêter leur activité et de se mettre en sécurité en quittant immédiatement leur lieu de travail.

Ce retrait doit s'exercer de telle manière qu'il ne puisse créer pour autrui une nouvelle situation de danger grave et imminent.

Aucune sanction ne peut être prise, aucune retenue de rémunération ne peut être effectuée à l'encontre d'agents qui se sont retirés d'une situation de travail dont ils avaient un motif raisonnable de penser qu'elle présentait un danger grave et imminent pour leur vie ou pour leur santé.

Il ne peut être demandé à l'agent qui a fait usage de son droit de retrait de reprendre son activité dans une situation de travail où persiste un danger grave et imminent résultant notamment d'une défectuosité du système de protection.

Chapitre II
Accès aux locaux et utilisation des moyens mis à disposition

Article 5 : Pour lui permettre l'accès aux locaux, il est remis, lors de son entrée en fonctions, à chaque agent un dispositif individuel. Ce dispositif ne peut être ni reproduit, ni cédé à un tiers.

Toute perte ou détérioration de ce dispositif est signalée sans délai au service de l'administration générale et des systèmes d'information. Ce dispositif est restitué lors de la cessation des fonctions.

Un agent ayant connaissance d'une atteinte portée aux locaux signale sans délai cette situation à son supérieur hiérarchique.

Article 6 : Le matériel informatique et téléphonique nécessaire à l'exécution de son travail est remis à l'agent lors de son entrée en fonctions.

Toute perte ou détérioration de ce matériel, y compris en télétravail, est signalée sans délai au service de l'administration générale et des systèmes d'information. Ce matériel est restitué lors de la cessation des fonctions.

Article 7 : Les règles relatives à l'utilisation des moyens informatiques mis à disposition par l'Agence sont déterminées par la charte d'usage du système d'information annexée à la présente décision.

Article 8 : La présente décision sera publiée sur le site internet de l'Agence.

La présidente
de l'Agence française de lutte contre le dopage,

Béatrice BOURGEOIS

Charte d'usage du système d'information

Toute personne ayant accès aux ressources informatiques de l'Agence, collaborateur ou tiers, désignées génériquement sous le terme d' « utilisateur », est tenue de se conformer à la présente charte.

La charte s'applique à tous les éléments du système d'information mis à la disposition des utilisateurs par l'Agence : matériels fixes ou portables, logiciels, systèmes de communication en interne ou en externe (messagerie, internet, téléphonie), informations et données quels que soient leurs supports (papier, numérique).

Conditions d'accès aux ressources informatiques et protection des équipements

Le matériel mis à disposition de l'utilisateur est strictement réservé à un usage professionnel.

Sauf autorisation préalable, il est interdit de mettre en place un équipement informatique qui pourrait interférer d'une quelconque manière avec les dispositifs informatiques, les solutions logicielles de travail ou l'infrastructure technique informatique de l'Agence. L'utilisation de supports de stockage personnels (clé USB, disque externe) est seulement tolérée à des fins d'échanges ponctuels.

L'utilisateur ne doit pas modifier la configuration de son poste de travail et des autres équipements mis à sa disposition par l'Agence sans l'accord du service en charge de la gestion du système d'information. En particulier :

- il n'ajoute pas et ne retire pas de composant matériel (disque dur, carte réseau, etc.) ;
- il n'installe pas de logiciels non autorisés par l'Agence ;
- il ne tente pas de modifier ou désactiver les mécanismes de protection (antivirus, paramétrage des mots de passe, installation des correctifs de sécurité, etc.) ;
- il ne tente pas de démarrer son poste de travail à partir d'un disque ou d'un autre support non autorisé (support externe, etc.) ;
- il ne cherche pas à répliquer les accès distants, en particulier la messagerie, à partir d'un équipement non maîtrisé par l'Agence.

Les moyens d'accès aux ressources informatiques, de quelque nature qu'il soit (mot de passe, certificat...) sont strictement personnels et incessibles. L'utilisateur respecte les règles en vigueur en termes de complexité et de renouvellement de ses mots de passe. Il accepte, le cas échéant, d'authentifier son accès par un autre moyen qui peut être personnel (comme l'application d'authentification sur un téléphone portable personnel).

L'utilisateur est responsable de la protection des équipements mis à sa disposition. En particulier :

- en cas d'absence, même momentanée, il verrouille ou ferme toutes les sessions en cours sur son poste de travail, sauf pour certains postes précis ;
- il 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, téléphone portable, etc.) ;
- il signale le plus rapidement possible au service en charge de la gestion du système d'information toute perte ou vol d'un équipement mis à sa disposition.

Protection des informations

Tout fichier, quel que soit son format (traitement de texte, archive électronique, script, exécutable...) à l'exception des fichiers identifiés comme « personnels », est réputé être la propriété de l'Agence. Tout fichier, document, courriel ou autre non expressément qualifié de « personnel » par l'utilisateur, quel que soit son support de stockage (serveur de fichiers, disques locaux d'un poste informatique de l'Agence,

messagerie électronique professionnelle...) peut donc être visualisé et exploité par l'Agence sans nécessiter l'accord de celui-ci.

L'utilisateur protège les informations placées sous sa responsabilité, en fonction de leur criticité. En particulier :

- il respecte la confidentialité des informations lors de toutes les phases de leur cycle de vie (stockage, transmission, impression, suppression, etc.). Il s'assure notamment que les informations confidentielles ou secrètes sont stockées et transmises de manière sécurisée ;
- il ne partage pas de données sensibles directement à partir de son poste de travail. Les échanges de fichiers entre utilisateurs doivent être réalisés *via* des services de l'Agence (serveur de fichiers, plateforme collaborative sécurisée) qui bénéficient des mécanismes de protection adéquats.

L'utilisateur reste vigilant quant au risque de divulgation d'informations sensibles dans l'espace public.

Utilisation des outils de communication

L'utilisateur demeure attentif lors de l'envoi de message. En particulier :

- il veille à ce que le contenu des messages qu'il envoie ne porte pas atteinte à l'image ou à la réputation de l'Agence ;
- il n'envoie pas ni ne fait suivre de message non sollicité (SPAM) ou contenant des informations illicites ou offensantes ;
- il ne met pas en œuvre des fonctions d'envoi ou de redirection automatique des messages lui étant destinés vers une adresse de messagerie dont les conditions d'exploitation et de sécurité ne sont pas contrôlées par l'Agence (à l'instar d'une adresse personnelle) ;
- il ne manipule jamais d'information contraire aux bonnes mœurs et à l'ordre public (accès à des sites Internet, stockage ou diffusion de fichiers, envoi de messages, etc.) sans impératif professionnel ;
- il ne communique jamais son adresse électronique professionnelle dans des circonstances sans rapport avec son activité professionnelle ;
- il n'engage pas à tort l'image de l'Agence, notamment dans le cadre d'interventions sur des forums ou des espaces de discussion.

L'utilisateur est vigilant lors de la consultation de sites qu'il ne connaît pas préalablement, en particulier des sites dont la notoriété n'est pas établie. Il prend toutes les précautions avant de télécharger toute pièce jointe depuis un site internet (format de la pièce, réputation du site...). En cas de doute, il consulte le service en charge de la gestion du système d'information de l'Agence.

L'utilisateur fait preuve de vigilance à l'égard des messages qu'il reçoit. En particulier :

- il n'ouvre pas les messages dont l'origine, l'objet ou le contenu sont douteux. Si une ouverture a été faite, il ne clique pas sur les liens ou les pièces jointes éventuellement insérés dans le corps du message ;
- il n'enregistre pas et n'exécute pas (notamment par double clics) les pièces jointes suspectes.

Intégrité du système d'information et mesures consécutives à un incident

L'utilisateur contribue, à son niveau, à la sécurité du système d'information. À ce titre, il signale tout dysfonctionnement ou tout événement lui apparaissant anormal. Le cas échéant, il met en application les règles et recommandations établies afin de résoudre ces dysfonctionnements.

L'Agence se réserve le droit d'analyser, de limiter et de contrôler l'utilisation des ressources matérielles et logicielles ainsi que les échanges, quelle que soit leur nature ou leur objet, effectués au moyen du système d'information de l'Agence, dans le respect de la règlementation en vigueur.

La journalisation des accès au système d'information de l'Agence (connexion à la messagerie, aux progiciels métiers, aux annuaires...) est mise en œuvre afin de pouvoir prévenir et analyser tout incident significatif.

Dans le cas de circonstances graves d'utilisations illicites ou mettant en cause le bon fonctionnement technique du système d'information, la sécurité ou les intérêts de l'Agence, le service en charge de la gestion des systèmes d'information de l'Agence pourra mettre en œuvre les actions de protection et/ou de correction nécessaires, et en informer le secrétaire général.

L'utilisateur peut demander au délégué à la protection des données la communication des informations nominatives le concernant et les faire rectifier conformément à la législation en vigueur. Pour ce faire, l'utilisateur doit envoyer un courriel précisant sa demande au délégué à la protection des données (dcp@afld.fr).