

Charte régissant l'usage des technologies de l'information et de communication

1. Préambule

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications pouvant être mis à disposition par le HCERES.

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les tablettes, les téléphones mobiles... est également un des éléments constitutifs du système d'information.

Par «HCERES», s'entend tout service du Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur.

Par «utilisateur», s'entend tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.

Ainsi sont notamment désignés :

- *tout agent titulaire ou non titulaire concourant à l'exécution des missions du HCERES (personnels administratifs, délégués scientifiques...)* ;
- *tout prestataire ayant contracté avec le HCERES.*

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte définit les règles d'usages et de sécurité que le HCERES et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

2. Engagements du HCERES

Le HCERES porte à la connaissance de l'utilisateur la présente charte.

Le HCERES met en oeuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

Le HCERES facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais le HCERES est tenue de respecter la vie privée de chacun.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie¹.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par le HCERES.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

¹ Notamment le secret médical dans le domaine de la santé.

Article 1 - Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent au HCERES ainsi qu'à l'ensemble des utilisateurs.

Article 2 - Conditions d'utilisation des systèmes d'information

2.01 – Utilisation professionnelle / privée

Les communications électroniques (messagerie, internet...) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques et peuvent constituer le support d'une communication privée.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement² à cet effet ou en mentionnant le caractère privé sur la ressource³. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

2.02 – Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur prévoit avec sa hiérarchie les modalités d'accès aux ressources du système d'information nécessaires à la bonne marche du service en son absence. Pour cela, le HCERES met à disposition de l'utilisateur les formulaires adéquats.

Si, en cas d'absence non planifiée et pour des raisons exceptionnelles, un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès⁴ au système d'information, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification à l'administrateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein du HCERES.

Article 3 - Principes de sécurité

3.01 – Règles de sécurité applicables

Le HCERES met en oeuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;

² Pour exemple, cet espace pourrait être dénommé "_privé_".

³ Pour exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique

⁴ Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité...).

- de garder strictement confidentiels son (ou ses) code(s) d'accès et ne pas le(s) dévoiler à un tiers (sauf cas prévus en section 2.02) ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

de la part du HCERES :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie (cf. section 2.02) ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

de la part de l'utilisateur :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par le HCERES ; les utilisateurs souhaitant utiliser leur matériel propre sont invités à prendre contact avec le service des systèmes d'information ;
- ne pas installer, télécharger ou utiliser sur le matériel du HCERES des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par le HCERES pour lutter contre les virus et les attaques par programmes informatiques.

3.02 – Devoirs de signalement et d'information

Le HCERES doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte, telle une intrusion dans le système d'information, etc. Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

3.03 – Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, le HCERES se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée, le cas échéant supprimée.

Le HCERES informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel.

Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions :

- lorsque ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;

- qu'elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;
- qu'elles ne tombent pas dans le champ de l'article⁵ 40 alinéa 2 du code de procédure pénale.

Article 4 - Communications électroniques

4.01 – Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein du HCERES.

Adresses électroniques

Le HCERES s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique⁶ nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins du HCERES.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'«utilisateurs», relève de la responsabilité exclusive du HCERES : ces adresses ne peuvent être utilisées sans autorisation explicite.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé⁷ ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés dans un guide technique d'utilisation de la messagerie qui est porté à la connaissance des utilisateurs.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui.

Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles⁸ 1369-1 à 1369-11 du code civil.

⁵https://www.legifrance.gouv.fr/affichCodeArticle.do?sessionId=B5F65545EFB0882820C41758AE863B27.tpdjo14v_1?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006574931&dateTexte=&categorieLien=cid (obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions...).

⁶ Pour exemple, l'adresse est de la forme prénom.nom@hceres.fr.

⁷ Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message.

⁸ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange, au même titre que pour les courriers traditionnels.

Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en oeuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation établi par le service ou le HCERES.

4.02 – Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension Intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors du HCERES.

Le HCERES met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques) : il peut constituer le support d'une communication privée telle que définie en section 2.02 dans le respect de la législation en vigueur.

En complément des dispositions légales en vigueur et au regard de la mission du HCERES, la consultation volontaire et répétée de sites à contenus de caractère pornographique depuis les locaux du HCERES est interdite.

Publications sur les sites internet et intranet du HCERES

Toute publication de pages d'information sur les sites internet ou intranet du HCERES⁹ doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé (pages privées...) sur les ressources du système d'information du HCERES n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le HCERES.

Sécurité

Le HCERES se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle *a priori* ou *a posteriori* des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par le HCERES.

L'utilisateur est informé des risques et des limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

4.03 – Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article 6.

Le HCERES se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information du HCERES, codes malveillants, programmes espions...).

Article 5 - Traçabilité

LE HCERES est dans l'obligation légale de mettre en place un système de journalisation¹⁰ des accès Internet, de la messagerie et des données échangées.

⁹ À partir des ressources informatiques mises à la disposition de l'utilisateur.

¹⁰ Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur...

LE HCERES se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Préalablement à cette mise en place, le prestataire du HCERES procédera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi n° 2004-801 du 8 août 2004.

Article 6 - Respect de la propriété intellectuelle

Le HCERES rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages Web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Article 7 - Respect de la loi informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée par la loi n° 2004-801 du 6 août 2004.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi «Informatique et Libertés».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.

Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'établissement dont il dépend.

Article 8 - Limitations des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement, la «personne juridiquement responsable» pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par «personne juridiquement responsable», on entend : toute personne ayant la capacité de représenter le HCERES.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles est passible de sanctions.

Article 9 - Entrée en vigueur de la charte

La présente charte est annexée au règlement intérieur du HCERES.