CHARTE
de bon usage des ressources numériques de l'Ecole des hautes études en santé publique

EHESP

Table des matières

1. Objet

Ce document, annexé au règlement intérieur de l'Ecole des hautes études en santé publique, est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs et des administrateurs en accord avec la législation applicable afin d'instaurer un usage correct et sécurisé des Ressources numériques et des services associés.
La Charte précise également les mesures de contrôle que l'EHESP met en œuvre pour s'assurer du respect de ces règles.

2. Champ d'application

La présente Charte s'applique à l'ensemble des agents de l'Ecole des hautes études en santé publique tous statuts confondus, les apprenants (élèves, étudiants) et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les ressources numériques de l'Ecole.
Elle sera signée et paraphée et/ou acceptée lors de la première connexion au système informatique par toute personne accueillie à l'Ecole des hautes études en santé publique et ayant accès au dit système.

3. Définitions

3.1.1. Le Système d'Information (SI)

Un Système d'Information peut être défini comme l'ensemble organisé de ressources (personnes, données, procédures, matériels, logiciels, etc.) permettant de traiter et diffuser de l'information en fonction des objectifs d'une organisation.

3.1.2. Ressources numériques

On désignera de façon générale sous le terme de Ressources numériques, l'ensemble des moyens technologiques délivrés par l'EHESP qui permettent le traitement d'information, qu'ils soient utilisés dans l'enceinte de l'école ou à l'extérieur et concoure de manière directe ou indirecte au fonctionnement du SI.

Les ressources numériques sont un élément du patrimoine de l'EHESP.

3.1.3. Utilisateur

Le terme Utilisateur désigne toute personne agissant sur le Système d'Information à titre permanent ou temporaire au moyen des ressources numériques qui lui sont mises à disposition par l'EHESP.

3.1.4. Administrateur

Le terme Administrateur désigne toute personne agissant sur le Système d'Information et disposant de privilèges d'accès supplémentaires du fait de ses missions.

On distingue deux types d'administrateur :

- Administrateur systèmes et/ou réseaux :

Il s'agit des personnes responsables du bon fonctionnement des ressources et services informatiques, et de leur sécurité.
Les administrateurs systèmes et réseaux sont localisés au sein de la Direction des Systèmes d'Information.

- Administrateur fonctionnel :

On désignera sous le terme «administrateur fonctionnel», toute personne responsable du bon fonctionnement d'applications spécifiques aux métiers ayant des droits de paramétrage sur les données et/ou les droits d'accès.

3.1.5. Responsable Sécurité du Système d'Information (RSSI)

Le Responsable de la sécurité du système d'information est le garant de la sécurité du SI et des données. A ce titre, il s'assure entre autres du respect des règles de la présente charte et assiste tout utilisateur dans l'interprétation et la compréhension des termes de celle-ci.

4. Règles d'utilisation des ressources numériques

4.1. Accès au SI

L'accès au SI de l'EHESP est soumis à l'autorisation d'accès basée sur une identification unique et sur un mot de passe que chaque utilisateur choisit seul, ne transmet à quiconque et dont il est le seul responsable. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers.

La connexion d'un équipement sur le réseau est soumise à autorisation préalable et doit respecter la politique de sécurité du Système d'Information.

Un Utilisateur ne peut en aucun cas permettre à une autre personne d'accéder au Système d'Information (SI) de l'Ecole au moyen de ses identifiants. Dans cette situation l'Utilisateur sera responsable des actions effectuées avec ses identifiants.

En cas de non-respect de cette Charte, les autorisations peuvent être annulées à tout moment. Toute autorisation d'accès et d'utilisation des Ressources numériques de l'Ecole prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

4.2. Ressources numériques

L'utilisation de Ressources numériques n'est autorisée que dans le cadre de l'activité professionnelle des Utilisateurs et dans la stricte conformité de la législation en vigueur et de la Charte RENATER.

Un usage à des fins non professionnelles est toléré sous réserve qu'il soit raisonnable et proportionné.

Tout Utilisateur a le devoir de s'informer et de respecter les règles de sécurité générales et spécifiques qui lui sont mises à disposition par l'EHESP (Intranet, sessions de sensibilisation, etc.).

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins non-professionnelles.

Notamment :

- Il doit appliquer les recommandations de sécurité de l'EHESP ;
- Il doit assurer la protection des informations qui lui sont confiées ;
- Il est responsable des droits qu'il donne aux autres Utilisateurs en particulier pour ce qui concerne les administrateurs techniques et fonctionnels ;
- Il lui appartient de protéger les données en utilisant les différents moyens de sauvegarde mis à sa disposition, l'Ecole n'est responsable que des données stockées sur ses serveurs ;
- Il doit signaler à son responsable, qui avisera le RSSI, toute tentative de violation de son compte et, de façon générale, toute anomalie ou incident de sécurité qu'il peut constater ;

- Il doit suivre les règles en vigueur au sein de l'EHESP pour toute installation de logiciel, par défaut aucune installation d'application qui ne serait pas validée par la DSIT n'est autorisée;
- Par ailleurs, l'Utilisateur ne doit ni installer, ni utiliser, ni stocker, ni publier, ni dupliquer, ni détourner de logiciel en l'absence de licence d'utilisation associée ou en l'absence d'autorisation du titulaire des droits de propriété intellectuelle dudit logiciel ;
- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
- Il ne doit pas tenter de lire, modifier, copier ou détruire des données sans l'accord explicite du propriétaire ;
- Il ne doit pas quitter son poste de travail ni ceux en libre-service laissant des ressources ou des services accessibles (verrouillage de la session, déconnexion) ;
- Il doit s'efforcer de réaliser ses missions professionnelles par le moyen le moins "coûteux" en ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseau, occupation de serveurs distants, etc.) ;
- Nul ne peut modifier la configuration d'une ressource numérique, sans un accord explicite de la DSIT.

4.3. Services Internet

L'Utilisateur doit faire un usage professionnel et raisonnable des services Internet, à ce titre il doit :

- respecter les règles de sécurité applicables au sein de l'EHESP ;
- respecter la législation en vigueur, notamment celles relatives à la propriété intellectuelle et aux publications portant atteinte à la dignité de la personne humaine.

Notamment :

- Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement du Système d'Information de l'EHESP ou d'un Système d'Information externe ;
- Il ne doit pas télécharger des logiciels ou des œuvres protégées sans autorisation ;
- Il ne doit pas usurper l'identité d'une autre personne ;
- Il ne doit pas intercepter des communications entre tiers et il a l'obligation de s'abstenir de toute ingérence dans la transmission des messages en vertu du secret des correspondances privées ;
- Il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Il veillera à ce que l'expression de ses opinions personnelles ne puisse porter préjudice à l'EHESP ou ne constitue pas un abus de droit d'expression ;
- Il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, pédophile, diffamatoire. De même, il doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents et les détruire en cas de réception fortuite.

4.3.1. Messagerie électronique

L'EHESP met à la disposition des utilisateurs concernés une boîte aux lettres électronique individuelle lui permettant d'émettre et de recevoir des messages électroniques.

L'utilisation d'une adresse nominative ou d'une adresse par délégation est de la responsabilité de l'Utilisateur.

L'utilisation de la messagerie institutionnelle :

- doit être professionnelle ou pédagogique ;
- s'effectue selon les normes définies par l'EHESP ;
- en conformité des modalités prescrites dans l'échelle de confidentialité.

Il est interdit d'utiliser un service de messagerie électronique tiers (ex : Yahoo, Gmail, …) dans le cadre professionnel.
Il est rappelé à l'Utilisateur que des échanges électroniques peuvent constituer des preuves et former un contrat. L'Utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il envoie ou qu'il échange.

L'EHESP tolère l'utilisation de la messagerie électronique à des fins personnelles dans le cadre des nécessités de la vie courante et familiale, dès lors que cet usage n'est pas abusif et n'entrave pas le trafic normal des messages professionnels.
S'il fait usage de cette faculté, l'Utilisateur est tenu d'indiquer, dans l'objet («subject») du message, la mention « Personnel » ou « Privé ».

A des fins de statistiques, de mesure de la qualité de service et de sécurité, le trafic de la messagerie est sujet à une supervision et à des vérifications et audits réguliers par l'EHESP.

L'emploi de listes de diffusion (GSEHESP notamment) doit être strictement réservé à un usage professionnel. Dans certains cas, une autorisation peut être nécessaire et une modération pourra être appliquée.

4.3.2. Réseaux sociaux

L'utilisation des réseaux sociaux dans le cadre de l'activité professionnelle de l'utilisateur doit satisfaire aux règles suivantes :

- ***Respect de l'audience :*** l'Utilisateur sera attentif à la façon dont il se présente et à la façon dont il communique. Il pourra exprimer ses points de vue et affirmer sa personnalité mais en veillant à toujours respecter son audience et rester fidèle à l'image de l'EHESP ;

- ***Honnêteté, transparence, responsabilité :*** L'Utilisateur est responsable de ce qu'il publie ou édite quel que soit le média utilisé. Il devra notamment s'assurer que l'ensemble des contenus qu'il publie sont libres de droit ou autorisés (image, vidéo, articles …). En cas d'utilisation de contenus associés à la marque EHESP (logo, images, vidéos, écrits…), il devra au préalable obtenir l'autorisation de la Direction de la communication ;

- ***Parler au nom de l'EHESP :***

  Dans les réseaux sociaux à usage externe et communautés virtuelles à usage personnel (Facebook, Linkedin, Twitter,...), seules les personnes habilitées peuvent s'exprimer au nom de l'EHESP sur les sujets concernant les activités de l'EHESP, la nature de ses services ou ses clients. S'il est habilité à s'exprimer au nom de l'EHESP, l'Utilisateur veillera à respecter en permanence dans ses communications les règles de confidentialité, les règles d'éthique et de comportement professionnel attachées à nos métiers, les obligations prévues par le contrat de travail de l'Utilisateur, et par le règlement intérieur de l'EHESP.

4.4 Utilisation de ressources numériques externes

Par défaut, l'utilisation de toute ressource numérique qui n'est pas délivrée ou qui n'est pas validée par l'EHESP est proscrite. Toutefois, sous réserve d'une validation préalable et explicite du RSSI, l'usage de ressource numérique externe peut être envisagée moyennant des recommandations et des limites d'usage (ex : à titre temporaire).

4.5 Informations, fichiers et données

La protection des données jugées sensibles porte sur toutes informations, produites, stockées, transmises au moyen des ressources numériques. Il s'agit entre autres des données à caractère personnel, des données scientifiques, …

Toute information produite par un utilisateur dans le cadre de son activité professionnelle au moyen des ressources numériques est la propriété de l'EHESP, sauf dans le cas d'une identification au moyen de la mention « Personnel » ou « Privé ».

L'accès par les Utilisateurs aux informations et documents conservés dans le Système d'Information doit être limité à ceux qui leur sont propres, publics ou partagés.

En particulier, il est interdit de prendre connaissance d'informations transitant sur les réseaux et détenues par d'autres Utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Cette règle s'applique également aux conversations privées de type courrier électronique dont l'Utilisateur n'est destinataire ni directement, ni en copie.

L'Utilisateur, soumis à une obligation de loyauté par application de l'article 1134 du Code civil et L.1222-1 du Code du travail, s'engage à ne pas qualifier de privés des fichiers ou dossiers professionnels.
Tout fichier ou dossier sans mention particulière (privé, personnel), est présumé avoir un caractère professionnel par l'EHESP et peut, à ce titre être consulté hors la présence de l'Utilisateur.

La diffusion de données personnelles n'est possible que dans le respect des prescriptions de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193).
Si, dans l'accomplissement de son travail, l'Utilisateur est amené à constituer des fichiers visés par la loi Informatique et Libertés, il devra auparavant s'être assuré de l'application de la procédure interne de sollicitation de la CNIL par l'Ecole.

4.6 Mobilité

Lors de l'utilisation de ressources numériques en dehors des locaux de l'EHESP, une vigilance accrue est attendue de la part de l'utilisateur, notamment vis-à-vis des risques de perte ou de vol. Il est attendu en particulier une attention soutenue à l'utilisation des ressources numériques dans les trains, gares et hôtels.

Il procède lui-même aux démarches rendues nécessaires (déclaration d'assurance, dépôt de plainte …) à la suite d'un incident, de quelque nature que ce soit ou d'un vol d'un matériel ou en cas de constat d'usurpation des éléments d'authentification et avise sans délai, le RSSI.

En cas d'incident avéré mais aussi en cas de doute, il doit immédiatement en aviser le Responsable Sécurité du Système d'Information.

4.7 Gestion des absences et droits d'accès

Chaque Utilisateur doit veiller à ce que la continuité du service soit assurée.
Afin d'éviter de laisser des messages professionnels sans traitement en cas d'absence, tout Utilisateur devra prévenir automatiquement ses interlocuteurs en proposant, dans la mesure du possible, une solution de remplacement (notification d'absence, redirection vers une adresse fonctionnelle).

4.8 Gestion des départs

Lors de son départ de l'EHESP, l'Utilisateur doit remettre, à sa hiérarchie et en bon état de fonctionnement, l'ensemble des moyens informatiques et de communication électronique ainsi que les moyens d'accès aux bâtiments ou services de l'EHESP mis à sa disposition dans le cadre de ses fonctions (ordinateur, périphériques, mobile, tablette, clé4G, abonnement téléphonique, supports de stockage, cartes d'accès, badges, …). Ces différentes ressources sont ensuite restituées aux différentes entités en charge de leur gestion.

Les comptes d'accès au Système d'Information et à la messagerie professionnelle sont désactivés le premier jour suivant le départ du personnel.
Sur demande explicite de l'Utilisateur, l'EHESP peut accorder une prolongation de 3 mois de l'accès à sa messagerie professionnelle.

A défaut et sauf procédure judiciaire ou enquête administrative, les répertoires ou documents « privé » ou « personnel » sont automatiquement supprimés, sans être consultés et sans qu'aucune copie ne soit réalisée.

5 Les règles applicables aux administrateurs

L'administrateur est soumis dans l'exercice de ses fonctions à un devoir de confidentialité pour assurer le bon fonctionnement et la sécurité du système d'informatique. Il peut procéder aux investigations nécessaires sur demande d'une autorité habilitée. Il est tenu de ne pas divulguer les informations acquises par ses recherches ou activités.

Par ailleurs l'administrateur :

- peut explorer les données des Utilisateurs et en faire connaître des extraits à son responsable ou sa direction générale lorsqu'une telle recherche est rendue nécessaire par le constat d'actes de malveillance et de piratage ;
- est tenu par la loi de générer tout journal d'évènements, et enregistrer des traces qu'il juge nécessaire afin de satisfaire à cette obligation ;
- n'est pas autorisé à accéder à toute donnée identifiée explicitement comme « personnelle » ou « privée » sans le consentement préalable de l'utilisateur concerné ;
- peut procéder à toute recherche préventive de faille sur l'ensemble du Système d'Information. Ils peuvent déconnecter, physiquement ou logiquement, un système en cas de suspicion ;
- de prendre, en cas d'infraction à la Charte, des mesures conservatoires, si l'urgence l'impose, sans préjuger des sanctions qui pourraient en résulter. Il en avertit, au plus vite, le Directeur du Système d'Information.

6 Contrôles et sanctions

6.4 Contrôle du respect des obligations

Les contrôles portant sur le respect des obligations auxquelles sont astreints les collaborateurs sont sous la responsabilité de leur hiérarchie.

L'EHESP s'assure du respect par l'Utilisateur de la réglementation en vigueur par la mise en œuvre des contrôles détaillés ci-après, notamment en matière de :

- Prévention et de répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou à l'ordre public ou de faits susceptibles de porter atteinte à la dignité d'autrui ;
- Prévention et de répression des atteintes aux droits de propriété intellectuelle d'autrui ;
- Prévention des actes liés à la sécurité des systèmes d'information : vol de données, dénis de service, altération de données, destruction, etc.

Les contrôles sont effectués dans le respect des dispositions légales et réglementaires en vigueur.

6.5 Analyse et contrôle de l'utilisation des ressources

6.5.1 Mesures de contrôle de l'utilisation d'internet

L'EHESP procède à des contrôles automatiques des flux sortants sur Internet. Contre toute utilisation abusive d'internet, l'EHESP utilise des moyens de contrôle du contenu des sites internet visités et le reporting des firewalls.
Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, l'EHESP constate un manquement à la Loi, la réglementation, au contrat de travail, à la Charte et aux prescriptions définies par note de service, elle se réserve le droit de procéder à l'identification de l'Utilisateur concerné.
Les données permettant d'identifier l'Utilisateur sont conservées pendant une durée de 1 an.
L'EHESP se réserve le droit de bloquer, sans information préalable, l'accès aux sites dont elle juge le contenu illégal, offensant ou inapproprié par des mesures de filtrage adaptées.

6.5.2 Mesures de contrôle de la messagerie électronique

L'EHESP réalise un suivi d'indices généraux des messages tels que le nombre, la volumétrie, les type de pièces jointes, etc.
Certaines mesures de contrôle plus spécifiques portant notamment sur la volumétrie et le nombre de mails échangés pourront être prises par l'EHESP vis-à-vis de ces messages.
L'EHESP utilise des outils de contrôle, de reporting et d'analyse du trafic.

Si l'EHESP présume un usage anormal ou interdit de la messagerie, elle procédera à l'identification de l'Utilisateur concerné.

6.5.3 Mesures de contrôle du trafic téléphonique

L'EHESP peut utiliser des moyens de suivi du trafic téléphonique des postes fixes ou logiciels et des téléphones mobiles qui permettent l'enregistrement des numéros des postes appelants et des numéros de téléphone appelés.
Les données enregistrées concernent le numéro appelant ou appelé, le jour et l'heure de l'émission ou de la réception de l'appel.
Des informations synthétiques concernant les téléphones fixes, mobiles et logiciels sont transmises périodiquement aux responsables de l'EHESP afin d'assurer le suivi des coûts.

6.6 Sanctions

Le présent document est porté à la connaissance de l'ensemble des personnels et apprenants dont chacun s'engage à en respecter toutes les dispositions.
Le non-respect d'une des clauses faisant partie des règles de bonne conduite et toute irrégularité dûment constatée pourront entraîner les sanctions prévues dans le Règlement Intérieur sans préjudice d'éventuelles sanctions de nature pénale ou professionnelle prévues par les textes en vigueur.

6.7 Rappel des principales lois françaises applicables

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique. À titre d'information et sans que la liste soit exhaustive, les obligations légales, réglementaires et contractuelles à prendre en considération peuvent être :

- Données à caractère personnel : Loi Informatique et Libertés du 6 janvier 1978, textes et publications de la CNIL, règlement européen 2016/679 du 27 avril 2016 sur la protection des données personnelles, surveillance de l'activité des agents et vie privée, accès aux données de l'agent, devoir de réserve, liberté d'expression ;
- Contrats, marchés et conventions : Arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics, textes relatives à la signature électronique présumée fiable (article 1316-4 du code civil), le code de la fonction publique, le code des marchés publics, Loi du 5 janvier 1988 dite loi Godfrain, etc. ;
- Propriété intellectuelle : respect des licences des produits et logiciels utilisés, loi HADOPI création et internet ;
- Législation française et européenne en matière de SSI : RGS, PSSI de l'État, LCEN (Loi n° 2004-575 du 21 juin 2004), Loi du 15 juillet 2008 relative aux archives publiques, règlement européen sur l'identification, l'authentification et la signature électronique « eIDAS », arrêté du 27 avril 2007 portant désignation des AQSSI, etc.