




Charte informatique agents et stagiaires du GIEP-NC



	« DEROULEMENT DES FORMATIONS »						PROCESSUS DE REALISATION N°2						
	« GESTION DES DOSSIERS ADMINISTRATIFS DES STAGIAIRES »						PROCEDURE N°11						
	« CHARTE INFORMATIQUE »						DOCUMENT N°9						
	Pilote du processus.		Alexandra CACELLI		Version.		2	Page(s).	11	AXE	2		
	Création.		Nov 17	Révision.		Avril 19	Validation.		Avril 19	Diffusion.		Avril 19	OBJECTIF
	Par.	JP GOLA	Par.	JP GOLA	Par.	G MUAVAKA	Par.	JP GOLA	CRITERE	19			



Sommaire

1. Règles générales et définitions	4
2. Respect des principes de fonctionnement des ressources informatiques et réseaux du GIEP-NC....	5
2.1. Usage professionnel	5
2.2. Sécurité informatique.....	5
2.2.1. Règles de définition et de gestion des mots de passe	5
2.2.2. Autres mesures de sécurité.....	6
2.2.3. Mesures de contrôle de la sécurité	6
2.2.4. Sécurité anti virale	7
2.3. Messagerie électronique	7
2.3.1. Généralités	7
2.3.2. Boîte aux lettres.....	7
2.3.3. Contenu des messages électroniques.....	7
2.3.4. Emission et réception des messages.....	7
2.3.5. Statut, valeur juridique et archivage des messages électroniques.....	8
2.4. Web, internet et traces	8
2.4.1. Règles complémentaires de sécurité liées à l'utilisation de l'internet	8
2.4.2. Téléchargements – Logiciels.....	8
2.5. Confidentialité et discrétion	8
2.6. Gestion des absences et des départs d'un utilisateur	9
3. Respect de la réglementation applicable en matière d'informatique et de communications électroniques	9
3.1. Propriété intellectuelle	9
3.2. Respect de la loi informatique et libertés.....	9
4. Dispositions finales	10
4.1. Limitations des usages	10
4.2. Application de la charte.....	10

I. RÈGLES GÉNÉRALES ET DÉFINITIONS

La présente charte a pour objet de formaliser les règles de déontologie et de sécurité que l'utilisateur s'engage à respecter en contrepartie de la mise à disposition des ressources informatiques du Groupement pour l'Insertion & l'Evolution Professionnelles (GIEP-NC).

Par « utilisateur », on entend : toute personne ayant accès, dans le cadre de l'exercice de son activité ou de sa formation professionnelle, aux moyens informatiques et de télécommunications quel que soit son statut et notamment :

- les agents titulaires et non titulaires, concourant à l'exécution des missions du GIEP-NC ;
- les stagiaires du GIEP-NC, dans le cadre de leur formation professionnelle ;
- les prestataires et le personnel des prestataires de service du GIEP-NC ;
- plus généralement toute personne (et notamment les invités) ayant accès au système d'information du GIEP-NC.

Par « système d'information », on entend : l'ensemble des moyens matériels, logiciels, applications et réseaux de télécommunications (Réseau Privé Virtuel, Réseau Téléphonique Commuté, etc..) pouvant être mis à disposition de l'utilisateur, y compris via l'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables...

L'utilisation du système d'information suppose le respect des règles visant à assurer la sécurité, la performance des traitements, l'intégrité et la préservation des systèmes et matériels, la protection des données confidentielles, et le respect des dispositions légales et réglementaires en vigueur.

Tout utilisateur est ainsi responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale ainsi qu'à celle de l'établissement pour lequel il travaille ou dans lequel il suit une formation.

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

En particulier:

- l'utilisateur doit appliquer les recommandations de sécurité du GIEP-NC ;
- il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition ;
- il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers ;
- il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage ;
- il ne doit pas utiliser des comptes autres que le sien ou masquer sa véritable identité ;
- il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles pour lesquelles il est autorisé à le faire. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification ;
- tout agent s'engage en quittant le groupement à ne pas modifier, détruire ou rendre inaccessible des données professionnelles sans l'accord explicite de son supérieur hiérarchique ;
- il ne doit pas quitter son poste de travail, ni ceux en libre-service, sans se déconnecter ;

- il ne peut modifier un équipement commun, tant du point de vue matériel que logiciel, ni connecter une machine au réseau sans l'accord explicite d'un représentant de la direction ;
- il ne doit ni installer ni utiliser de logiciels à caractère ludique ;

L'utilisateur est informé que la violation des procédures régissant l'accès et l'utilisation du système d'information et de télécommunication mis à sa disposition est susceptible d'entraîner des mesures conservatoires, poursuites et/ou sanctions, tant internes que pénales.

Les règles de déontologie et de sécurité figurant dans la présente charte, de même que l'obligation de respecter la législation en vigueur s'appliquent à l'ensemble des utilisateurs du système d'information du GIEP-NC.

2. RESPECT DES PRINCIPES DE FONCTIONNEMENT DES RESSOURCES INFORMATIQUES ET RÉSEAUX DU GIEP-NC

2.1. Usage professionnel

Les moyens informatiques, fixes ou nomades, mis à disposition de l'utilisateur sont destinés à un usage professionnel. L'utilisation à des fins privées est toutefois tolérée, doit être non lucrative et limitée tant dans la fréquence que dans la durée, conformément aux conditions et limites figurant dans la présente Charte.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat ainsi qu'aux obligations qui lui incombent en raison de la nature même de ses fonctions.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard des coûts d'exploitation globaux.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé (messages, lettres, carnets d'adresses etc.) dans un espace de données nommé « privé » et/ou « personnel », espace qui ne sera alors pas (systématiquement) inclus dans les sauvegardes. Toutes les informations ne se trouvant pas dans cet espace privé sont réputées professionnelles. Ainsi, la sauvegarde régulière de ses données privées incombera à l'utilisateur, sous sa seule responsabilité.

Il est rappelé à l'utilisateur qu'en aucun cas, l'utilisation du système d'information à des fins privées ne doit avoir pour effet de nuire à la qualité de son travail ni au temps qu'il y consacre, ni au bon fonctionnement du service.

2.2. Sécurité informatique

Les niveaux d'accès de l'utilisateur sont définis en fonction du profil utilisateur qui est établi pour chacun selon les critères propres à son statut, sa mission, la nature de son poste et ses besoins professionnels. Paramétrage et mots de passe sont des éléments essentiels de cette sécurité globale.

2.2.1. Règles de définition et de gestion des mots de passe

La sécurité des moyens informatiques mis à la disposition de l'utilisateur lui impose :

- de respecter les consignes de sécurité et notamment les règles relatives à la définition et aux changements des mots de passe ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mot de passe d'un autre utilisateur, ni chercher à connaître ces informations ;
- de garder strictement confidentiels ses mots de passe et ne pas les dévoiler à un tiers ; de changer immédiatement ses mots de passe en cas de doute sur leur confidentialité.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouvait dans l'obligation de communiquer son mot de passe, il devra procéder, dès qu'il en a la possibilité, au changement de ce dernier ou en demander la modification à l'administrateur du réseau. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.

L'utilisateur est informé que les mots de passe constituent une mesure de sécurité destinée à éviter les utilisations malveillantes ou abusives. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Chaque utilisateur est personnellement responsable du mot de passe qu'il choisit.

2.2.2. Autres mesures de sécurité

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions.

La sécurité des ressources mises à la disposition de l'utilisateur nécessite :

- de verrouiller son poste de travail en cas d'absence et/ou d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail ;
- d'avertir immédiatement ou dans le délai le plus court, sa hiérarchie de tout dysfonctionnement constaté, de toute anomalie découverte, telle une faille de sécurité, une intrusion dans le système d'information, de tout accès à une ressource informatique ne correspondant pas à son habilitation etc. ;
- de ne pas modifier l'équipement qui lui est confié en conformité avec les dispositions en vigueur du groupement ;
- de ne pas installer, télécharger ou utiliser sur les matériels informatiques de logiciel ou progiciel sans qu'une licence d'utilisation appropriée n'ait été souscrite ;
- de s'interdire d'accéder ou tenter d'accéder à des ressources ou programmes informatiques pour lesquels l'utilisateur ne bénéficie pas d'une habilitation expresse. L'utilisateur doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toutes autres, même si cet accès est techniquement possible.

L'utilisateur est informé que pour des actions de maintenance corrective ou évolutive, l'administration du système d'information a la possibilité de réaliser des interventions, le cas échéant à distance, sur les ressources mises à sa disposition.

2.2.3. Mesures de contrôle de la sécurité

Le système d'information ainsi que l'ensemble des moyens de communication peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Ainsi, l'ensemble des données relatives au trafic, tel que précisé par le Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, peuvent être conservées pendant une durée n'excédant pas 1 an.

Les personnels en charge de ces opérations sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsque ces informations sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur.

2.2.4. Sécurité anti virale

L'utilisateur se conforme aux règles liées à la mise en œuvre au sein de l'institution, des dispositifs de lutte contre les virus et attaques logiques informatiques.

L'utilisateur est informé que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée voire détruite. Dans la mesure du possible, il reçoit un message l'avertissant de cette opération.

Les services réseaux pourront être arrêtés en cas de difficultés majeures, même sans préavis.

2.3. Messagerie électronique

2.3.1. Généralités

Le groupement met à la disposition de ses agents une boîte à lettres professionnelle nominative qui lui permet d'émettre et de recevoir des messages électroniques.

L'élément nominatif de l'adresse de la messagerie qui constitue le prolongement de l'adresse administrative, n'a pas pour effet de retirer le caractère professionnel de la messagerie.

Les messages envoyés ou reçus faisant l'objet d'une limitation de taille, le message est rejeté et l'émetteur reçoit un message de non distribution, en cas de dépassement de la taille limite.

2.3.2. Boîte aux lettres

Chaque utilisateur peut autoriser, à son initiative et sous sa responsabilité, l'accès par des tiers à sa boîte de réception.

L'attribution de boîtes générales fonctionnelles ou organisationnelles par service ou groupe d'utilisateurs est possible.

Les listes de diffusion institutionnelles désignant une catégorie ou un groupe d'utilisateurs ne peuvent être mises en place et utilisées que sous la condition d'une autorisation de l'institution.

2.3.3. Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité directe du groupement. En toutes circonstances, l'utilisateur doit adopter un comportement loyal, digne et respectueux.

Tout message à caractère privé, reçu ou émis, doit comporter une mention particulière explicite indiquant le caractère privé en objet. A défaut, le message sera réputé professionnel sauf s'il est stocké dans un espace privé de données. Un message privé est soumis au secret de la correspondance privée.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place, comme la limitation en volume de pièce jointe au message.

Sont notamment interdits les messages à caractère injurieux, raciste, discriminatoire, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, l'appartenance syndicale, la santé des personnes, ou encore, de porter atteinte à leur vie privée ou à leur dignité ainsi que les messages portant atteinte à l'image, la réputation ou à la considération du GIEP-NC.

2.3.4. Emission et réception des messages

Il incombe à l'utilisateur de s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

La diffusion des messages est limitée aux seuls destinataires concernés afin d'éviter la diffusion de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

L'utilisateur informe ses correspondants du caractère professionnel de sa messagerie, en leur spécifiant que :

- Tout message à caractère strictement privé, émis, doit comporter en objet la mention « Privé » ou tout autre terme indiquant sans ambiguïté le caractère privé du message ;
- Tout message ne comportant pas cette mention est réputé être un message professionnel.

2.3.5. Statut, valeur juridique et archivage des messages électroniques

Rappel : Les messages électroniques échangés avec des tiers, particulièrement des commerçants (cf article L. 110-3 du Code de commerce), peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve.

L'utilisateur est en conséquence vigilant sur la nature des messages électroniques qu'il échange au même titre que les courriers traditionnels, ainsi que sur la conservation des messages pouvant être nécessaire en tant qu'éléments de preuve.

2.4. Web, internet et traces

2.4.1. Règles complémentaires de sécurité liées à l'utilisation de l'internet

L'accès à internet n'est autorisé qu'au travers des dispositifs de sécurité, et navigateurs sélectionnés et paramétrés mis en place par le groupement.

L'utilisateur qui dispose d'un accès au réseau internet est informé des risques et limites inhérents à son utilisation.

Le groupement a mis en place un système permettant d'assurer la traçabilité des accès Internet et/ou des données échangées ; et se réserve le droit de procéder à un filtrage des sites, au contrôle à posteriori des sites, des pages visitées et durées des accès correspondants.

2.4.2. Téléchargements – Logiciels

Le téléchargement de fichiers, notamment de sons et d'images, depuis le réseau internet est autorisé s'il correspond à l'activité professionnelle de l'utilisateur, dans le respect des droits de la propriété intellectuelle.

Cependant, le groupement se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux et/ou comporter des virus susceptibles d'altérer le bon fonctionnement du système d'information.

2.5. Confidentialité et discrétion

Chaque utilisateur a une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel auxquels il a accès dans le système d'information.

Le respect de cette confidentialité implique notamment :

- de veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;
- de respecter les règles d'éthique professionnelle et de déontologie, ainsi que l'obligation de réserve et le devoir de discrétion.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations 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. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup

de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec l'autorité investie du pouvoir de nomination.

2.6. Gestion des absences et des départs d'un utilisateur

En cas d'absence d'un utilisateur, les mesures strictement nécessaires visant à assurer la continuité du service pourront être mises en œuvre par la hiérarchie, dans le respect de la vie privée et du secret des correspondances de cet utilisateur.

Il appartient à l'utilisateur, lors de son départ définitif du service ou du groupement, de détruire son espace « privé ».

Les espaces privés d'un utilisateur quittant le service ou le groupement, s'ils n'ont pas été détruits par ce dernier, n'engagent pas la responsabilité du groupement quant à la conservation et la confidentialité de ces dites données.

3. RESPECT DE LA RÉGLEMENTATION APPLICABLE EN MATIÈRE D'INFORMATIQUE ET DE COMMUNICATIONS ÉLECTRONIQUES

3.1. Propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle du groupement, de ses partenaires et plus généralement de tous tiers titulaires de tels droits.

Chacun doit donc :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier et 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.

3.2. 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 nominatives conformément à la loi n° 78-17 modifiée du 6 janvier 1978 dite « Informatique et Libertés ».

Par données nominatives, il y a lieu d'entendre, les 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, notamment quand il s'agit de données nominatives « sensibles », y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi du 6 janvier 1978.

En conséquence, tout utilisateur souhaitant procéder à un tel traitement, par l'intermédiaire de sa direction devra préalablement demander et obtenir l'autorisation de la CNIL. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

Par ailleurs, il est rappelé que, conformément aux dispositions de la loi informatique et libertés n°78-17 du 6 janvier 1978 modifiée, 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.

4. DISPOSITIONS FINALES

4.1. Limitations des usages

En cas de non-respect des lois et règlements en vigueur, ainsi que des règles définies dans la présente Charte, la direction du GIEP-NC pourra, sans préjuger des poursuites ou procédures de sanctions pénales et/ou disciplinaires pouvant être engagées à l'encontre des agents, limiter les usages par mesure conservatoire.

4.2. Application de la charte

La présente charte s'applique à l'ensemble des agents du GIEP-NC tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques du GIEP-NC.

Le GIEP-NC se réserve le droit, dans le respect de la législation applicable, de contrôler le respect des dispositions de la présente charte en accédant aux fichiers assurant la traçabilité des actions menées par chaque utilisateur.

Je soussigné(e), madame, mademoiselle ou monsieur (1)
..... reconnais avoir reçu un exemplaire de la présente charte et avoir compris ce document que je m'engage à respecter. Je suis informé que la violation des règles et procédures exposées dans ce document est susceptible de m'exposer à des sanctions.

Fait à, le

Signature.

(1) Rayer la mention inutile et indiquez vos nom et prénom et lettres capitale