Seine-Maritime
Le Département

Convention concernant la sécurisation des échanges Entre le Département de Seine-Maritime et les utilisateurs du e-CLHD

Entre :

Le Département de Seine Maritime, représenté par son Président en exercice, autorisé par délibération de la Commission Permanente du 23 septembre 2013

Ci-après nommé : le Département

Et

La Ville de Rouen contributeur au site e-CLHD

Ci-aprés nommé : Ville de Rouen

Vu la loi n° 2006-872 du 13 juillet 2006 portant engagement national pour le logement ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu la désignation du Correspondant à la protection des données du Département de Seine-Maritime à la CNIL le 20 janvier 2008;

Vu le décret n°2012-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2005 relatif à la sécurité des informations échangées par voie électronique ;

Vu l'arrêté du 6 mai 2010, dit arrêté RGS, portant approbation de la première version du référentiel général de sécurité ;

Vu la délibération n° 2.2 de la Commission Permanente du Département de Seine-Maritime du 21 janvier 2013 relative à l'évolution de la politique générale de protection de l'information et à la nouvelle charte de sécurité informatique et du bon usage des ressources informatiques, électroniques et numériques

Vu la déclaration du traitement intitulé « gestion du comité local habitat dégradé » réalisée par le Département de Seine-Maritime auprès de son Correspondant à la protection des données à caractère personnel ;

Vu la délibération du Conseil Général du 11 décembre 2007 relative aux interventions départementales en faveur de l'habitat privé –lutte contre l'habitat dégradé ;

Vu la délibération du Conseil Général du 14 octobre 2008 adoptant le 4e Plan Départemental d'Action pour le Logement des Personnes Défavorisées ;

Vu l'avis favorable du Comité Responsable du Plan du 22 juin 2009 pour la création des Comités locaux Habitat Dégradé ;

Vu la délibération de la Commission Permanente du 23 septembre 2013 autorisant le Président à signer la présente convention ;

Il est convenu ce qui suit

Article 1 : Préambule

Le comité local habitat dégradé (CLHD) constitue un lieu unique d'observation de toutes les situations d'habitat dégradé (non décent et indigne) et de traitement de celles-ci.
Son rôle est de rendre le travail du Département et des partenaires plus efficace en leur donnant la possibilité, sur un même dossier, et de manière simultanée, de décider d'apporter des recommandations sinon partagées, du moins coordonnées, sur les solutions à mettre en œuvre.
Ainsi, un site collaboratif externe a été créé afin de faciliter l'accès aux informations relatives aux différents CLHD, d'améliorer le partage d'information entre la Direction de l'Aménagement et de l'Habitat du Département et les utilisateurs dans une logique de simplification des procédures administratives et de dématérialisation. La mise en œuvre de cet espace partagé, facilement accessible, sécurisé, interactif et évolutif, a donc pour vocation de fédérer les différents acteurs du Département et des partenaires autour de la thématique de l'habitat dégradé.
Le site collaboratif susvisé, désigné e-CLHD constitue un système d'information permettant d'échanger par voie électronique des informations entre plusieurs autorités administratives. Il doit donc de facto se conformer aux principes du référentiel général de sécurité (RGS), établi par le décret n°2010-112 du 2 février 2010 et en vigueur depuis l'arrêté du Premier Ministre du 6 mai 2010.
La présente convention définit les modalités de transfert des données entre le Département et la Ville de Rouen ainsi que les modalités de leurs mises à jour.

Article 2 : Objet de la convention

La présente convention a pour objet de garantir la sécurité des échanges entre les différents utilisateurs, nommément habilités, du site collaboratif e-CLHD, en fixant les modalités de fourniture et de diffusion des données mentionnées dans le présent article.

Ces modalités concernent :

- les modalités de mise à jour des données par l'ensemble des utilisateurs habilités et définies à l'article 3 ;
- le partage de l'information générale à savoir la mise en ligne de documents de communication au format Acrobat pdf, des dates des instances du comité local habitat dégradé, des sessions de formation, des études de l'observatoire départemental de l'habitat dédiées à l'habitat dégradé ;
- le suivi des signalements;
- le partage des documents de travail de manière interactive;
- la simplification et la rationalisation des travaux du secrétaire du comité local habitat dégradé et du chargé de mission de l'observatoire départemental de l'habitat ;

- l'élaboration d'un espace par territoire de CLHD afin de limiter l'accès aux informations partagées (sous-sites sécurisés et ciblés, ordres du jour territorialisés, relevés de recommandations territorialisés) ;
- la sécurité des échanges entre le Département et la Ville de Rouen.

Article 3 : Les données saisies

Le Secrétariat-animation du comité local habitat dégradé (CLHD), l'observatoire départemental de l'habitat (ODH) et les membres utilisateurs du site collaboratif e-CLHD pour les dossiers les concernant s'engagent à saisir les données suivantes à partir d'une grille de signalement ou d'informations fournies par le Responsable social ou le chargé de mission logement du Département :

- les caractéristiques du logement de l'occupant (numéro INSEE, adresse, étage, caractéristiques de l'immeuble, typologie du logement, statut ;
- l'identité de l'occupant (nom et prénom) ;
- l'identité du propriétaire (nom et prénom) ;
- la date du signalement ;
- l'identité du déclarant du signalement (nom et prénom) ;
- la situation de l'occupant et du propriétaire ;
- le numéro d'allocataire CAF de l'occupant ;
- la composition de la famille (nombre d'adultes, de mineurs, d'enfants de moins de 6 ans) ;
- l'adresse complète du propriétaire ;
- la nature du signalement ;
- la qualification suspectée de la situation ;
- la problématique du bâti ;
- la qualification avérée de la situation ;
- le contexte social via la saisie de cases à cocher « oui/non » ;
- la problématique juridique via la saisie de cases à cocher « oui/non ».

Article 4 : Obligations générales du Département et la Ville de Rouen

Le Département et la Ville de Rouen s'engagent au respect des dispositions de la loi n° 78 - 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 et à celles du référentiel général de sécurité (RGS).

La Ville de Rouen membre du comité local habitat dégradé (CLHD) et utilisateur habilité du site collaboratif e-CHLD s'engage à respecter les conditions de protection de l'information précisées dans la charte de sécurité informatique et du bon usage des ressources informatiques, électroniques et numériques du Département de Seine-Maritime et dans la politique générale de protection de l'information du Département de Seine-Maritime (PGPI).

Les parties à la présente convention conviennent que ces documents seront mis en ligne sur le site collaboratif e-CLHD.

Seuls pourront avoir accès au site collaboratif e-CLHD des agents nommément désignés par le responsable de la Ville de Rouen, ayant préalablement signé le récépissé de prise de connaissance de la charte de sécurité informatique et du bon usage des ressources informatiques, électroniques et numériques du Département de Seine-Maritime. En cas de départ ou de changement d'affectation d'un agent habilité, le responsable de la Ville de Rouen s'engage à en informer sans délai le Département pour que les droits d'accès à l'application soient supprimés et la sécurité des données garanties.

Le Département et la Ville de Rouen reconnaissent être tenus à une obligation générale de conseil, d'information et de recommandation, tout au long de la durée de la présente convention.
La Ville de Rouen s'engage à ce que les informations fournies par Département de Seine-Maritime ne puissent être utilisées à d'autres fins que celles prévues dans la présente convention.
A cet égard, la Ville de Rouen s'oblige à assurer la protection de toutes les données fournies par le Département de Seine-Maritime.

Article 5 : Clause relative à la protection des données à caractère personnel

Les supports informatiques fournis par le Département et tous documents de quelle que nature qu'ils soient résultant de leur traitement par la Ville de Rouen restent la propriété du Département.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226.13 du code pénal). Conformément aux articles 34 et 35 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Ville de Rouen s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La Ville de Rouen s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel, c'est-à-dire notamment à :

- ne prendre aucune copie des documents et supports d'informations confiés par le Département de Seine-Maritime et utilisés par la Ville de Rouen à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet de la présente convention ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées à la présente convention ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution de la convention ;
- prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée de la présente convention ;

et au terme de la convention à :

- procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies ;

ou à :

- procéder à la destruction des données à caractère personnel contenues dans les fichiers ;

ou à :

- restituer intégralement les supports d'informations selon les modalités prévues à la présente convention.

Les supports d'informations qui lui seront remis devront être traités sur le territoire français métropolitain.
En cas de sous-traitance, ces dispositifs seront pleinement applicables au sous-traitant.

Le Département de Seine-Maritime se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la Ville de Rouen.

Il est rappelé que, en cas de non respect des dispositions précitées, la responsabilité de la Ville de Rouen peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du code pénal.

Le Département de Seine-Maritime pourra prononcer la résiliation immédiate de la convention, sans aucune indemnité, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Article 6 : Rôles du Département et la Ville de Rouen

Tel qu'en dispose la loi n°78-17 modifiée du 6 janvier 1978, le Département est, pour le traitement « site collaboratif e-CLHD », responsable de traitement (cf. article 3 loi n°78-17 modifiée) et la Ville de Rouen les sous-traitant (cf. article 35 loi n°78-17 modifiée). La Ville de Rouen agit donc pour le compte du responsable du traitement et selon ses instructions.

Article 7 : Aménagements de la présente Convention

La présente Convention peut être modifiée ou complétée par voie d'avenants, soumis à l'approbation de la Commission Permanente du Département et de l'organe délibérant de la Ville de Rouen.
En cas de non-respect des engagements réciproques inscrits dans la présente convention, celle-ci pourra être résiliée de plein droit par l'une ou l'autre des parties, à l'expiration d'un délai de quinze jours suivant l'envoi d'une lettre recommandée avec accusé de réception, valant mise en demeure.

Article 8 : Avenants

Toute modification des conditions ou modalités d'exécution de la présente convention, définie d'un commun accord entre les parties à la présente convention, fera l'objet d'un avenant. Celui-ci précisera les éléments modifiés de la convention, sans que ceux-ci puissent conduire à remettre en cause les objectifs généraux de la présente convention.

Article 9 : Règlement des litiges

En cas de litige résultant de l'interprétation ou de l'application de la présente convention, les parties à la présente convention s'engagent à tout mettre en œuvre pour parvenir à un règlement amiable dudit litige.
En cas d'échec de conciliation, le différent sera porté devant le tribunal compétent.

Article 10 : Durée de la Convention

La présente Convention est conclue pour une durée correspondant à celle du fonctionnement des CLHD et du site e-CLHD.

Fait à Rouen
en 2 exemplaires

Le Président du Département
Pour le Président et par délégation,
La Vice-Présidente du Département

Christine RAMBAUD

Le Maire

Yvon ROBERT

Annexes :

- Politique générale de protection de l'information du Département de Seine-Maritime
- Charte de sécurité informatique et du bon usage des ressources informatiques, électroniques et numériques du Département de Seine-Maritime

Charte Utilisateurs des Ressources Informatiques

Rédaction	Vérification	Approbation
S. BONENFA NT	DP	D.G.S

Date : 28 mai 2008

Avant-propos :

SOMMAIRE

1. Objectif du document

La présente Charte a pour objet d'exposer les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre dans l'utilisation du Système d'Information.

Elle complète la définition des principes généraux de sécurité du Système d'Information du Département exprimée dans le document « Politique de sécurité du Système d'Information du Département de Seine-Maritime ».

Selon les règles et procédures définies par le Département, il est mis à disposition de tout utilisateur des moyens techniques de traitement de l'information (notamment le poste de travail informatique et ses périphériques, imprimantes, serveurs des plates-formes, téléphone ...).

A ces moyens techniques sont associés des droits liés à la mise en œuvre des applications et services (progiciels, messagerie, Intranet, espaces communs, Internet..) et des droits liés au traitement des données et informations. Les droits d'accès, de modification, de stockage, de destruction, d'exécution ou de communication sont attribués en fonction de l'activité professionnelle des utilisateurs.

Chaque utilisateur doit être conscient que :

- L'usage du système d'Information obéit à des règles qui s'inscrivent dans le respect de la loi, de la déontologie et de la sécurité du Département (sauvegarde du patrimoine et des intérêts du Département).
- L'ouverture d'un réseau informatique constitue toujours un risque pour la sécurité.
- La négligence ou la mauvaise utilisation de ces systèmes font encourir des risques au Département et à lui même.

Tout utilisateur contribue donc à la sécurité générale du Système d'Information :

La présente Charte appelle à une attitude loyale, courtoise, responsable et respectueuse d'autrui, dans l'intérêt du Département et de l'ensemble des personnes qui y travaillent.

Elle est aussi rédigée dans l'intérêt de chacun des utilisateurs du SI et doit permettre d'assurer un développement harmonieux de l'accès de chacun à ce SI, dans le respect des lois et règlements en vigueur, en particulier ceux relatifs au respect de la vie privée et au secret des correspondances visés par les articles 9 du code civil et 226-15 du code pénal.

2. Domaine d'application

La présente Charte est applicable à l'ensemble des personnes ayant un accès au Système d'Information du Département de Seine-Maritime :

- Agents du Département ;
- Elus du Département ;
- Personnel externe (prestataires, stagiaires, sous-traitants) ;
- Partenaires (élus et agents d'autres collectivités territoriales, agents de la fonction publique d'état, collaborateurs d'associations).

Les modalités d'accès aux ressources par les organisations syndicales et leurs correspondants ainsi que leur utilisation au profit des agents font l'objet de dispositions figurant dans un protocole spécifique, publié sur l'intranet.

La présente charte est disponible sur l'Intranet du Département (Vie de l'agent./ Environnement professionnel) :

Charte utilisateurs des ressources informatiques

3. Principes de base

Les principes de base sont les suivants :

R1. L'utilisateur est responsable de l'usage qu'il fait des ressources informatiques et du réseau auxquels il a accès.

R2. L'utilisateur doit consacrer l'usage de son environnement de travail (moyens techniques et droits) à son activité professionnelle.

R3. Un usage personnel raisonnable est toutefois admis pour répondre à des nécessités de la vie courante et/ou familiale.

Cet usage doit être conforme aux obligations (de réserve, discrétion et neutralité) des fonctionnaires :

R4. Il ne doit pas être contraire à l'ordre public et aux bonnes mœurs.

R5. Il ne doit pas mettre en cause l'intérêt et la réputation du Département et doit se faire dans le respect des lois, notamment celles relatives aux publications à caractère injurieux, raciste, pédophile, pornographique ou diffamatoire

L'utilisateur est responsable de l'environnement de travail qui lui est attribué et de l'usage qui en est fait. A ce titre, il a le devoir de :

R6. Respecter les dispositions légales, celles de la présente charte, et les procédures, consignes et règles propres à son site

R7. S'interdire de produire, de collecter ou de transmettre des données, messages ou œuvres en infraction avec la législation en vigueur, notamment les messages contraires à l'ordre public, diffamatoires, racistes, xénophobes, portant atteinte à la décence ou constituant une diffusion de fausses nouvelles.

R8. S'engager à prendre toutes dispositions pour consulter ou reproduire de manière licite les données ou œuvres protégées par des droits d'auteur, sous quelque forme que ce soit, notamment les logiciels, les oeuvres audiovisuelles et littéraires.

R9. Respecter les contraintes techniques qui lui sont indiquées.

R10. Prendre toutes les précautions utiles afin de préserver la sécurité des informations traitées et notamment empêcher qu'elles ne soient déformées, endommagées, indisponibles ou encore communiquées à des tiers non autorisés.

R11. Signaler immédiatement, à son responsable hiérarchique et au Responsable Sécurité des Systèmes d'Information (RSSI), toute anomalie constatée, tout incident de sécurité ou suspicion d'incident.

Préalablement à ce signalement, l'utilisateur procédera à la déconnexion de son ordinateur du réseau par retrait de son câble d'attachement réseau.

4. Règles d'utilisation

4.1 Messagerie

La messagerie est un moyen de communication extrêmement utilisé, mais absolument pas sécurisé. L'utilisateur doit être conscient que :

- l'adresse d'émission peut être usurpée ;
- le message peut être adressé en copie cachée à certains destinataires ;
- le message peut être intercepté pour en connaître son contenu et son émetteur ;
- tout message émis depuis le réseau du Département transporte l'identité du Département (cg76.fr) et donc implique celui-ci via son contenu ;
- le contenu du message peut être altéré ;
- les fichiers attachés sont des vecteurs d'infections ;
- des messages trop volumineux ou trop fréquents saturent le réseau du Département.

L'utilisateur doit donc utiliser la messagerie à bon escient et respecter les règles et recommandations édictées ci-après.

4.1.1 Limitation de la volumétrie

4.1.1.1 Pour les échanges de messages

L'utilisateur veillera à adapter et limiter aux besoins ses messages, tant en contenu qu'en nombre de destinataires, et utilisera tous les moyens techniques mis à sa disposition pour en réduire la taille, tels que :

- la compression éventuelle des pièces jointes ;
- l'insertion des liens hypertexte ;
- l'utilisation appropriée des listes de diffusion ;
- ...

4.1.1.2 Pour le stockage

L'utilisateur veillera à limiter la conservation de messages reçus et émis en respectant la règle suivante :

R12. Supprimer les messages anciens devenus inutiles et archiver régulièrement les messages professionnels importants sur l'espace de stockage mis à disposition sur le réseau.

4.1.2 Utilisation à titre privé

Il doit être considéré qu'un message reçu ou envoyé depuis le poste de travail mis à disposition par le Département, revêt un caractère professionnel.

Toutefois, sont considérés comme messages privés :

- les messages comportant dans leur objet la mention « privé » ou « personnel » ;
- les messages classés dans un dossier créé par l'utilisateur et nommé « privé » ou « personnel » ;
- les échanges non professionnels avec les organisations syndicales, les services sociaux, les services médicaux ...

4.1.3 Parades aux risques extérieurs

Afin de faire face aux problématiques sécuritaires telles que citées plus haut, les règles suivantes sont à respecter :

R13. Aucune messagerie instantanée par connexion à Internet (du type ICQ, AOL Messenger, Yahoo Messenger, etc.) ne doit être utilisée, sauf exception dûment signalée.

R14. N'ouvrir que les pièces jointes des messages dont l'émetteur est connu.

R15. Ne pas donner suite aux demandes de redIffusion de messages alarmistes ou de suppression de fichiers.

4.2 Accès Internet

Une vigilance particulière est demandée dans l'utilisation de certains services sur Internet. L'utilisateur doit être conscient que :

- une page web contient des données et du code exécutable (normal et/ou malveillant) ;
- le téléchargement de logiciels douteux peut amener une infection informatique voire une attaque du Département ou de ses agents ;
- la navigation peut générer à l'insu de l'utilisateur une surcharge du trafic sur le réseau de l'entreprise (voire le bloquer) ;
- toute requête issue du réseau du Département vers un site web transporte l'identité du Département et donc implique celui-ci ;
- la navigation génère des « cookies » (fichiers spécifiques) permettant de connaître les consultations effectuées et les centres d'intérêts de l'utilisateur.

L'utilisateur doit donc utiliser le web en respectant les règles et recommandations ci-après :

R16. Certains usages, fortement consommateurs de ressources réseau (vidéo, visioconférence, ...) peuvent faire l'objet de restriction, voire d'interdiction.

R17. L'accès à des services Internet doit se faire au moyen des protocoles HTTP ou HTTPS.

R18. La participation à des forums est interdite, sauf exception devant faire l'objet d'une demande de dérogation auprès de la Direction Générale des Services.

R19. L'envoi de fichiers vers Internet au moyen du protocole FTP ainsi que l'échange de fichiers entre ordinateurs personnels (« peer to peer » externe) sont interdits, sauf exception dûment signalée.

R20. Pour des besoins particuliers, l'utilisateur formule sa demande à la DSI, après visa de sa hiérarchie.

R21. Il est formellement interdit de télécharger ou installer depuis Internet des programmes inconnus (notamment les fonds d'écran, les utilitaires de navigation, etc.) ainsi que des pièces jointes sur de la messagerie personnelle, de type « yahoo.fr » ou « hotmail.com ».

NB : Certains sites Internet pouvant être régis par des règles juridiques autres que de droit français, toutes les précautions doivent être prises à cet égard par l'utilisateur.

4.3 Configurations matérielles et logicielles

Les composants techniques mis à disposition de l'utilisateur pour ses activités professionnelles font l'objet, par le Département, de mesures techniques de sécurité,

Les règles suivantes sont à respecter :

R22. Sauf s'il y est autorisé, l'utilisateur ne doit pas modifier les périphériques et les logiciels de communication qui lui sont fournis ou installer de nouveaux équipements non agréés, notamment des modems et des points d'accès Wifi.

R23. Les seules configurations matérielles et logicielles autorisées sont celles mises à la disposition par la DSI du Département. La DSI du Département se réserve le droit de remettre en conformité tout équipement qui dérogerait à la règle.

R24. Les équipements non fournis par la DSI du Département (ordinateurs portables, PDA,..) ne doivent pas être connectés au réseau.

R25. Ne pas désactiver la fonction de mise à jour du logiciel antivirus, ni désinstaller le logiciel.

R26. L'utilisateur d'un ordinateur portable est tenu de se connecter fréquemment au réseau départemental pour permettre l'exécution des mises à jour des configurations systèmes et antivirus de ses équipements.

R27. À l'intérieur des locaux du Département, l'utilisateur d'un ordinateur portable ne doit utiliser que la prise du réseau local du Département et non celle réservée au téléphone analogique au moyen d'un modem, ou encore une carte de connexion sans fil (3G/GPRS, WiFi, ...) ;

R28. Un ordinateur portable est plus exposé qu'un ordinateur de bureau du fait de sa miniaturisation. Son utilisateur doit veiller à ne pas l'exposer à la chaleur

ou à des différences de température importantes, notamment dans les transports. Il doit le préserver des chocs, en le transportant systématiquement avec sa housse.

4.4 Droits d'accès et protection des données

L'utilisateur protège son environnement de travail, les données et les informations auxquelles il a accès ou qu'il diffuse, par l'emploi adapté des moyens de protection mis à sa disposition.

4.4.1 Diffusion de l'information

Par ailleurs, il ne peut accéder qu'aux seules informations et documents qui lui sont propres, et qui sont publics ou partagés.

Les règles suivantes sont à respecter :

R29. Pour toute information disponible dans les systèmes d'information du Département, l'utilisateur doit s'assurer de la possibilité de diffusion avant toute communication à l'extérieur (règles définies par les services ou autorisations spécifiques).

R30. Tout message électronique comportant dans l'adresse de l'expéditeur l'identification du Département émetteur engage, si ce n'est la responsabilité de celui-ci, du moins son image. En conséquence, l'utilisateur doit respecter les règles de validation et le formalisme fixés par l'autorité hiérarchique dont il dépend.

R31. Faire preuve d'une obligation de réserve (vis-à-vis de l'extérieur, comme à l'intérieur du Département) puisqu'il y a engagement de l'image du Département. Lorsque l'utilisateur s'exprime à titre personnel, il doit l'indiquer de manière explicite.

R32. S'assurer de la possibilité de diffusion avant toute communication à l'extérieur. Lorsqu'il s'exprime à titre personnel, l'utilisateur doit l'indiquer explicitement.

4.4.2 Accès à l'information

Sauf mesures particulières prévues pour des nécessités de service, il est interdit de prendre connaissance et d'utiliser des informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Les droits d'accès sont attribués nommément à un utilisateur et n'ont pas vocation à être cédés, afin de préserver l'accès aux ressources contre des tiers non autorisés.

Les règles suivantes sont à respecter :

R33. Les mots de passe doivent être robustes, gardés secrets, et ne doivent en aucun cas être communiqués.

R34. Ne pas quitter son poste de travail (ou un poste en libre-service) sans verrouiller ou quitter la session de travail.

R35. Pour certaines applications sensibles, des dispositions d'authentification forte (clé USB, carte à puce) ont été délivrées. L'usage de ces dispositifs est personnel et ne doit en aucun cas faire l'objet d'un prêt.

R36. Il est fortement recommandé aux utilisateurs d'ordinateurs portables de protéger le démarrage de ceux-ci avec un mot de passe (dans le SETUP ou le BIOS).

R37. À l'extérieur des locaux du Département, un ordinateur portable ne doit pas être laissé sans surveillance, ni être confié à un tiers, y compris un proche (conjoint, enfants, etc).

4.4.3 Stockage de l'information

Le Département met à la disposition de tout utilisateur un espace de stockage sur le réseau, pour le stockage de ses données professionnelles (et uniquement celles-ci), dont le contenu est sauvegardé tous les jours.

R38. Il appartient à l'utilisateur de protéger ses données en utilisant les espaces de stockage mis à sa disposition sur le réseau (espace disque personnel dûment attribué).

4.4.4 Respect des droits d'accès

L'utilisateur ne peut accéder qu'aux seules informations et documents qui lui sont propres, et qui sont publics ou partagés :

R39. Ne pas utiliser ou essayer d'utiliser des comptes autres que le sien, ni masquer sa véritable identité, ni utiliser des informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

R40. Il est interdit d'effectuer toute action visant à observer le trafic réseau, sans autorisation du Responsable de la Sécurité des Systèmes d'Information.

4.4.5 Données d'un utilisateur absent

Les règles suivantes sont à respecter :

R41. Tout Directeur doit définir les règles d'accès aux applications ou aux données bureautiques de sa Direction et leur partage entre les utilisateurs intéressés.

R42. A l'exception des messages marqués « privé » dans leur objet ainsi que des messages vocaux dans leur globalité et des parties du disque dur réservées à l'usage personnel de chaque utilisateur (nommée« documents privés », par exemple), les données accessibles depuis le poste de travail ou contenues sur les micros ordinateurs fournis par le Département peuvent

être consultées, en l'absence de l'utilisateur intéressé, sur la demande de son Directeur.

5. Contrôle de l'utilisation

Tout utilisateur a droit au respect de ses données privées. Toutefois, il doit être conscient que les systèmes informatiques enregistrent et peuvent mémoriser les transactions et les informations de connexion.

5.1 Accès aux traces

Seuls les administrateurs techniques et les personnels habilités au titre de la sécurité disposent d'outils d'analyse, de surveillance et de contrôle. Tenus au secret professionnel, ils ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni les intérêts du Département. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

Tout traitement automatisé d'informations nominatives dont l'objet est la sécurité du système d'information, le suivi, le contrôle de l'utilisation des ressources informatiques et des services Internet doit faire l'objet d'une déclaration à la CNIL et être soumis à son contrôle.

5.2 Modalités de contrôle

Dans le cadre de ce traitement et suivant la gravité de l'anomalie constatée, seul le Directeur Général des Services du Département peut donner son accord préalable à un contrôle individuel détaillé. L'utilisateur concerné est immédiatement informé par écrit du contrôle.

Les modalités d'exercice des contrôles en cas d'anomalie sont les suivantes :

R43. L'autorité hiérarchique compétente pour autoriser un contrôle individuel détaillé est le Directeur Général des Services du Département.

R44. Le contrôle individuel détaillé n'est réalisé qu'après l'information écrite préalable de l'utilisateur concerné et son acceptation ; une information orale peut être également réalisée mais elle ne constitue pas un élément suffisant d'information.

R45. Les suites données aux constatations réalisées font l'objet également d'une information écrite faite à l'utilisateur concerné.

6. Règles de mise en œuvre de la charte

6.1 Respect des obligations de la charte

La mise en oeuvre de cette charte répond aussi bien aux besoins du Département qu'à ceux des utilisateurs.

Les manquements qui seraient regardés comme des fautes professionnelles sont susceptibles d'entraîner pour l'utilisateur des sanctions disciplinaires sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

6.2 Suivi et révision de la charte

Le suivi annuel et la révision de la charte feront l'objet d'une procédure concertée avec les représentants du personnel.

Les règles suivantes seront appliquées :

R46. La présente Charte sera remise à chaque utilisateur du Système d'Information du Département, via sa hiérarchie.

R47. Elle sera remise à tous les nouveaux agents ou élus du Département.

R48. Elle sera disponible en consultation sous une ressource partagée (intranet,...).

R49. Le recours à des collaborateurs occasionnels ou à des personnes extérieures au Département nécessite que ces utilisateurs reçoivent toutes les informations utiles quant à leurs droits et obligations issus de la présente Charte. A cette fin, la Charte sera annexée à leur contrat de travail ou bien notifiée dans le cadre de la procédure contractuelle qui lie ces personnes au Département.

R50. La charte sera ajoutée au programme de sensibilisation à la sécurité des systèmes d'information.

7. Principaux textes législatifs applicables

- Code civil, art. 9 (respect dû à la vie privée)
- Code pénal, notamment art.226-13 à 226-14 (atteintes au secret professionnel), 226-15 (atteinte au secret des correspondances), 226-16 à 226-24 (atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques), 323-1 à 323-7 (atteinte aux systèmes de traitement automatisés de données)
- Loi du 1er Juillet 1992 relative au Code de la propriété intellectuelle
- Loi du 29 juillet 1881 sur la liberté de la presse, notamment le chapitre IV
- Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et les actes réglementaires pris en application de son article 15 pour autoriser la mise en oeuvre de traitements informatiques
- Loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment art.6 (liberté d'opinion), 8 (droit syndical) et 26 (obligations de discrétion et de secret professionnels, auxquelles sont rattachées les obligations de réserve et de neutralité)
- Loi n°84-16 du 11 janvier 1984 modifiée portant obligations statutaires relatives à la fonction publique de l'Etat
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
- Loi du 5 janvier 1988 dite « Godfrain » relative à la fraude informatique.
- Loi (646) du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications
- Code du travail :
  - Principe de proportionnalité (L1121-1)
  - Information préalable du Comité d'entreprise sur la mise en œuvre de moyens de contrôle des salariés (L1221-9 et 1222-4)
  - Obligation d'informer le salarié ou candidat à l'emploi sur les dispositifs informatisés le concernant (L2323-13, L2323-14 et L2323-32)
  - Consultation du Comité d'entreprise pour introduction de nouvelles technologies modifiant les conditions de travail (L2323-13, L2323-14 et L2323-32)
- Loi du 15 novembre 2001 relative à la sécurité quotidienne (LSQ)

8. Glossaire

BIOS (Basic Input Output System ou **système élémentaire d'entrée/sortie**) : ensemble de fonctions, contenu dans la mémoire morte de la **carte mère** servant à faire des opérations basiques (écrire un caractère à l'écran, lire un **secteur** sur un disque, etc...).

CNIL (Commission Nationale de l'Informatique et des Libertés) : Autorité administrative indépendante française chargée de veiller à la protection des données personnelles et à la protection de la vie privée. Elle a été créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Cookies : Petits fichiers textes stockés par le navigateur Web sur le disque dur du visiteur d'un site Web et servant (entre autres) à enregistrer des informations sur le visiteur (exemple : identifiant et mot de passe) ou encore sur son parcours dans le site.

FTP (File Transfer Protocol : protocole de transfert de fichiers) : Protocole de communication dédié à l'échange informatique de fichiers. Il permet en particulier, depuis un ordinateur, de copier des fichiers depuis ou vers un autre ordinateur du réseau.

GPRS (General Packet Radio Service) : Norme pour la téléphonie mobile permettant un débit de données élevé. On le qualifie souvent de 2,5G : intermédiaire entre la 2^{ième} (GSM) et la 3^{ième} génération (UMTS).

HTTP (HyperText Transfer Protocol) : Protocole de communication utilisé par les navigateurs pour accéder à un serveur Web.

HTTPS : Variante sécurisée de HTTP (avec S pour « Secured », soit « sécurisé »).

PDA (Personal Digital Assistant ou *assistant personnel ou ordinateur de poche*) : Appareil numérique portable.

Peer to Peer (réseaux poste à poste) : Permet à plusieurs ordinateurs de communiquer, de partager simplement des informations --des fichiers le plus souvent, sans passer par un serveur spécifique.

Les systèmes poste à poste sont accusés de servir essentiellement à la distribution de fichiers multimédias sans respect des droits d'auteurs ou de diffusion.

RSSI : Responsable de la Sécurité des Systèmes d'Information d'une organisation (entreprise, association ou institution). Il est responsable du maintien du niveau de sécurité du système d'information.

SETUP : Programme permettant l'installation et l'initialisation d'un composant matériel ou logiciel sur un ordinateur.

WiFi : Technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à Internet.

Seine-Maritime
Le Département

RECEPISSE (Cas des recrutements) A JOINDRE AU DOSSIER DE RECRUTEMENT

NOM :

Prénom :

Direction :

Service :

Déclare avoir bien pris connaissance de la charte des utilisateurs des ressources informatiques

Date :

Signature de l'agent

« Le département de Seine-Maritime met en place un traitement destiné à suivre les retours de récépissés de prise de connaissance de la charte utilisateurs des ressources informatiques. Conformément à la loi «informatique et libertés» du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au Correspondant Informatique et Libertés du Département de Seine-Maritime (cil@cg76.fr). »

Seine-Maritime
Le Département

RECEPISSE (Cas des agents, des élus et du personnel externe du Département de Seine-Maritime) A ENVOYER AU :

CORRESPONDANT A LA PROTECTION DES DONNEES

NOM :

Prénom :

Direction :

Service :

Déclare avoir bien pris connaissance de la charte des utilisateurs des ressources informatiques

Date :

Signature de l'agent

« Le département de Seine-Maritime met en place un traitement destiné à suivre les retours de récépissés de prise de connaissance de la charte utilisateurs des ressources informatiques. Conformément à la loi «informatique et libertés» du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au Correspondant Informatique et Libertés du Département de Seine-Maritime (cil@cg76.fr). »

RECEPISSE (Cas des partenaires du Département de Seine-Maritime) A ENVOYER AU :
Correspondant à la Protection des Données
Département de Seine-Maritime
Direction Générale des Services
Quai Jean Moulin
76101 ROUEN Cedex

NOM :

Prénom :

Organisation :

Direction :

Déclare avoir bien pris connaissance de la charte des utilisateurs des ressources informatiques

Date :

Signature de l'agent

« Le département de Seine-Maritime met en place un traitement destiné à suivre les retours de récépissés de prise de connaissance de la charte utilisateurs des ressources informatiques. Conformément à la loi «informatique et libertés» du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au Correspondant Informatique et Libertés du Département de Seine-Maritime (cil@cg76.fr). »