Pays
Cœur d'Hérault

CHARTE INFORMATIQUE

Document source

Comité Technique Départemental

Service Statuts-Rémunération du Centre de Gestion d'Ille-et-Vilaine

Dispositions applicables aux collectivités territoriales

SOMMAIRE

INTRODUCTION

L'objectif

La présente charte informatique formalise les règles d'usage et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein du SYDEL Pays Coeur d'Hérault.

Le manquement à la présente charte pourra entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/ et/ou des sanctions pénales.

Le champ d'application

La présente charte s'applique à **l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire.**
Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques du SYDEL Pays Coeur d'Hérault. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.

Dés l'entrée en vigueur de la présente charte, chaque agent du SYDEL Pays Coeur d'Hérault s'en verra remettre un exemplaire.

I - LES REGLES GENERALES D'UTILISATION

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom du SYDEL Pays Coeur d'Hérault qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de bienséance.

A - Les droits et les devoirs des utilisateurs

Un accès aux ressources réglementé
Toute personne travaillant dans la collectivité dispose d'un droit d'accès au système d'information.
Ce droit d'accès est :

- Strictement personnel.
- Incessible.

Une utilisation professionnelle des ressources
Les ressources informatiques mises à disposition constituent un outil de travail nécessaire. Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter l'intégrité et la confidentialité des données.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi « informatique et liberté » du 06/01/1978). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives.
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de "ressources extérieures" matérielles ou logicielles.

- Respecter les contraintes liées à la maintenance du système d'information.

B - Les droits et les devoirs du SYDEL Pays Coeur d'Hérault

- *LA DECLARATION OBLIGATOIRE :*

La loi "Informatique et Libertés" impose une déclaration préalable auprès de la Commission Nationale de l'informatique et des libertés" (CNIL) de tout traitement automatisé d'informations nominatives permettant l'identification directe ou indirecte d'une personne.

- *L'INFORMATION INDIVIDUELLE :*

L'employeur peut satisfaire à cette obligation par la diffusion de tous documents précisant les règles d'usage de son système d'information ainsi qu'à leur application (charte informatique, règlement intérieur, note de service...).

- *LA DISPONIBILITE ET L'INTEGRITE DU SYSTEME INFORMATIQUE :*

La collectivité s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources,...) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

C – L'analyse et le contrôle

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique et de l'autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés.

D - Les sanctions

La Loi, les textes réglementaires (cf. pages 10 et 11) et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.
Tout utilisateur du système d'information du SYDEL Pays Coeur d'Hérault n'ayant pas respecté la loi pourra être poursuivi pénalement (cf. pages 10 et 11)

E - Les évolutions

La présente charte pourra être complétée ou modifiée par l'assemblée délibérante après avis du comité technique. Un avenant sera alors délivré à l'ensemble du personnel pour informatiion.

II - LES POSTES INFORMATIQUES

- Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition de chaque utilisateur :
  - Matériel : unité centrale, écran, clavier, souris...,
  - Système d'exploitation : Windows 7 ou 10,
  - Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats.

- Toute installation logicielle est à la charge du responsable informatique.

- En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches 'Ctrl+Alt+Suppr' et cliquer sur 'Verrouiller l'ordinateur').
- En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller son PC.
- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran et l'imprimante.
- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers.
- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations stockées sur les serveurs ou les NAS.
- L'utilisateur doit signaler tous dysfonctionnements ou anomalies au responsable informatique par courriel ou appel téléphonique.
- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire des espaces de stockage.
- Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

*L'employeur a accès au contenu d'une **clé USB** personnelle connectée à l'ordinateur professionnel. Dés lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur, la clé USB appartenant au salarié est présumée utilisée à des fins professionnelles, de sorte que l'employeur peut avoir accès aux fichiers non-identifiés comme personnels qu'elle contient, hors la présence du salarié.*

III – LA MESSAGERIE

- L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels. La lecture des courriels personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle.

- L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect. (cf annexe : 5 reflexes à avoir lors de la réception d'un courriel)

- Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'Autorité Territoriale ou le responsable informatique (même en l'absence de l'utilisateur). Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel et confidentiel » dans leur objet. Ces derniers ne pourront alors être ouverts par l'Autorité territoriale ou le responsable informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la Loi.

- L'utilisateur s'engage à ne pas envoyer en dehors des services du SYDEL Pays Coeur d'Hérault des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

- L'utilisateur signera tout courriel professionnel.

- L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.

- L'utilisateur doit vérifier le contenu et l'historique des messages transférés *(gestion du "Répondre à tous").*

- L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Il utilisera à bon escient l'indicateur d'urgence (poit d'exclamation rouge accompagnant les messages hautement prioritaires) Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier

« éléments supprimés » doit être vidé périodiquement. Il s'engage à limiter le volume des mails stockés.

- En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.

- La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par la collectivité.

- Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (ordonnance n° 2005-1516 du 8 décembre 2005). Ils doivent, en conséquence être traités dans les mêmes délais.

IV – LES SITES INTERNET

- L'utilisation d'Internet est réservée à des fins professionnelles.

- Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

- L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédo-pornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).

- Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

- Le stockage permanent sur les postes de données téléchargées sur Internet est interdit.

- Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

- Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'Autorité territoriale.

- Pour éviter les abus, l'Autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

- Toute saisie d'informations sur un site Internet professionnel nécessite l'autorisation préalable de l'Autorité territoriale.

- Toute procédure d'achats personnels sur Internet est formellement interdite.

- L'utilisation de forums de discussion est autorisée pour un usage professionnel.

V – LES RESEAUX SOCIAUX

- L'utilisation des réseaux sociaux est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels. La consultation des comptes personnels durant les heures de travail est tolérée si celle-ci reste occasionnelle.
- L'utilisation doit être appropriée et doit respecter le devoir de réserve.

- Des autorisations de communication sur les réseaux sociaux sont attribuées aux agents, aux services, qui sont habilités à parler au nom du SYDEL Pays Coeur d'Hérault.
- La distinction entre l'utilisation professionnelle et l'utilisation personnelle est recommandée (création de deux profils)
- Les conditions d'utilisation et d'accès sont définies (restrictions et limites pratiques).

VI – LE TELEPHONE

Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.

Règles d'utilisation

- L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone fixe pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle.

- L'Autorité territoriale peut procéder au contrôle de l'ensemble des appels émis depuis les téléphones professionnels.

- En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique.

- L'agent qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel.

- L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

VII – LE SMARTPHONE (fourni par l'employeur)

- Le smartphone est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels) sous réserve d'autorisation préalable et strictement définie.

- Il n'est pas obligatoire de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congés). Les téléphones portables doivent être restitués lors des absences prolongées (au-delà d'une semaine).

- Le smartphone ne doit pas venir perturber une réunion ou un entretien qui sont des évènements sociaux qui nécessitent la présence physique et intellectuelle de chacun.

VIII – LES BASES LEGALES

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

La Réglementation

- **Loi n° 78-17 du 06/01/1978** sur l'informatique, les fichiers, les libertés.

Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

- **Loi n° 78-753 du 17/07/1978** sur la liberté d'accès aux documents administratifs.

Loi portant diverses mesures d'amélioration entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

- **Loi n° 85-660 du 03/07/1985** sur les droits d'auteur et la protection des logiciels.

Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

- **Loi n° 91-646 du 10/07/1991** relative au secret des correspondances émises par voie de télécommunication

- **Loi n° 2000-230 du 13/03/2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

- **Loi n° 2004-575 du 21/06/2004** pour la confiance dans l'économie numérique.

Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

- **Loi n°2012-410 du 27/03/2012** relative à la protection de l'identité.

Le Code Pénal

Code Pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

- **Article 323-1** :
« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60.000 euros d'amende.
- **Article 323-2** :
« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-3** :
« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-4** :
« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

- **Article 323-5** :
« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics.
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

- **Article 323-6** :
« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :
1° L'amende, suivant les modalités prévues par l'article 131-38.
2° Les peines mentionnées à l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

- **Article 323-7** :
« La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines. »

Annexe

5 réflexes à avoir lors de la réception d'un courriel

N'importe qui peut vous envoyer un courriel en se faisant passer pour un autre ! Cela n'est pas beaucoup plus compliqué que de mettre un faux nom d'expéditeur au verso d'une enveloppe.

1 - N'ayez pas une confiance aveugle dans le nom de l'expéditeur

Soyez donc attentif à tout indice mettant en doute l'origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude, par exemple. En cas de doute, contactez votre interlocuteur pour vérifier qu'il est à l'origine du message.
Et même si l'expéditeur est le bon, il a pu, à son insu, vous envoyer un message infecté.
Vous devez admettre que dans le domaine de la messagerie électronique, il n'existe pas d'expéditeur a priori de confiance.

2 - Méfiez-vous des pièces jointes

Elles peuvent contenir des virus ou des espiogiciels.
Assurez-vous régulièrement que votre antivirus est activé et à jour.
Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites-le contrôler.

3 - Ne répondez jamais à une demande d'informations confidentielles

Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande car vous pouvez être victime d'une tentative de filoutage, ou phishing. Il s'agit d'une technique utilisée par des personnes malveillantes, usurpant généralement l'identité d'un tiers ou simulant un site dans lesquels vous avez a priori confiance (une banque, un site de commerce, etc.) dans le but d'obtenir des informations confidentielles, puis de s'en servir.
Les messages du type chaîne de lettres, porte-bonheur ou pyramide financière, appel à solidarité, alerte virale, ou autres, peuvent cacher une tentative d'escroquerie. Évitez de les relayer, même si vous connaissez l'expéditeur.

4 - Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur

En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur. Dans la plupart des tentatives de filoutage, notamment lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont d'un niveau très moyen, et les caractères accentués peuvent être mal retranscrits. Toutefois, on constate qu'un nombre croissant de tentatives de filoutage emploie un français correct. Soyez donc le plus vigilant possible lors de la réception de tels messages.

5 - Paramétrez correctement votre logiciel de messagerie

paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des courriels ;
dans un environnement sensible, lisez tous les messages au format texte brut.

Recommandations de l'ANSSI - L'Agence Nationale de la Sécurité des Systèmes d'Information
www.ssi.gouv.fr