COMMUNAUTÉ URBAINE DE BORDEAUX

LA CUB

DÉPLACEMENTS
ENVIRONNEMENT
URBANISME
DÉVELOPPEMENT ÉCONOMIQUE

PROJET

CHARTE DE BON USAGE DES RESSOURCES DU SYSTEME D'INFORMATION

Sommaire

1. Préambule

Le développement des réseaux et l'utilisation croissante des technologies de l'information induisent, progressivement, une nouvelle forme d'organisation et de gestion des relations au sein des administrations, et à l'égard des usagers grâce, par exemple :

- à la mise en ligne d'informations pour plus de transparence,
- à la mise en place d'Intranets pour une meilleure communication entre les agents et les services,
- à la mise en place d'Extranets (Intranet d'agglo…) dans le cadre de partage d'informations *avec des partenaires / usagers*.

Cette évolution expose le système d'information (SI)* de la CUB à de nouveaux risques (infections par des virus, attaques externes, vols d'informations, …) et le rend plus vulnérable, d'où l'enjeu de sa protection.

La mise en œuvre des dispositifs organisationnels et techniques est ainsi complémentaire avec la vigilance de chacun.

La méconnaissance de la législation, l'ignorance des risques encourus ou une mauvaise application de règles parfois simples et de bon sens, mais toujours essentielles, peuvent être lourdes de conséquence pour la CUB, comme pour chaque agent dans la mesure où sa propre responsabilité pourrait être également engagée.

Cette charte est un guide.

Son application au quotidien est l'affaire de tous, dans l'intérêt de chacun.

2. Objet

Cette charte s'applique à l'ensemble des moyens de communication (systèmes d'information, téléphonie, imprimantes, copieurs…), quelle que soit la forme sous laquelle ils sont exploités (électronique, imprimée, manuscrite, vocale, image …).

Elle a pour objet :

- de **faire prendre conscience de la problématique sécuritaire et de responsabiliser chaque utilisateur*, individuellement,**
- de **mettre en évidence la nécessité, pour la sécurité de tous, de respecter cette charte,**
- de **clarifier les droits, les devoirs et les responsabilités des utilisateurs (élus, agents communautaires, prestataires…),**
- d'**adopter les comportements de sécurité qui sont nécessaires.**

Les principes énoncés ne sont pas exclusifs de l'application des lois, des devoirs (statut, devoir de probité*…) incombant aux agents, et des règles minimales de courtoisie et de respect d'autrui.

* Définition à l'article 10

3. Champ d'application

Ensemble des ressources du SI:

- applications métiers, bureautiques, messagerie, Internet, intranet, extranet,
- données,
- PC fixes, PC portables, périphériques notamment imprimantes, clés USB, scanners, …
- assistants personnels,
- téléphones fixes, mobiles (GSM, postes TETRA),
- fax, photocopieurs
- appareils photo numériques.
- …

Ensemble des utilisateurs du SI :

- agents stagiaires et titulaires,
- élus, collaborateurs de groupes d'élus,
- collaborateurs de cabinet,
- stagiaires écoles,
- agents contractuels (de droit public, de droit privé, apprentis) et les personnes intervenant dans le cadre de vacations,
- prestataires,
- partenaires : Syndicats, COS, ASSCUB,…
- ….

4. Législation

La loi s'appliquant à tous, chaque utilisateur peut être tenu pour responsable civilement ou pénalement dans sa mission au quotidien, en cas de manquement à ses obligations légales et réglementaires. En être conscient permet de mieux assumer ses responsabilités.

La Responsabilité de principe du chef d'établissement ne couvre pas la responsabilité individuelle des agents.

Selon la loi, l'utilisateur DOIT	**Selon la loi, l'utilisateur NE DOIT PAS**

- **Respecter les règles applicables à la fonction publique territoriale :**
  - secret professionnel,
  - obligation de réserve,
  - devoir de discrétion, …
 	
- **Respecter les règles relatives à la protection des données nominatives,** notamment les informations relatives à la matrice cadastrale, …
 	
- **Répertorier les fichiers de données à caractère personnel** et transmettre les informations nécessaires à la DSI en vue d'une déclaration à la **CNIL.**
	- **Chercher à porter** atteinte directement ou indirectement **aux droits des personnes physiques (comme morales) ainsi qu'à leur vie privée,** (protection des libertés individuelles et des personnes, respect du secret des correspondances).
	
	- **Se rendre coupable**, directement ou indirectement, quel que soit le moyen (informatique, téléphonique, courrier, …), de **délits dits « de presse »** (diffamation, injure …) ou procéder au stockage de documents proscrits par la loi (détention d'images ou de textes à caractère pédophile ou raciste …).

Selon la loi, l'utilisateur DOIT	Selon la loi, l'utilisateur NE DOIT PAS

- **Respecter les règles de protection du droit d'auteur** en ne se rendant pas coupable de contrefaçon :
  - à l'occasion d'un téléchargement de données (marque, son, image, texte …) depuis un site Internet,
  - en faisant une **copie d'un logiciel commercial** pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle,
  - en photocopiant sans autorisation des documents protégés (articles de presse, livres, …) à des fins autres que privées.
- **N'utiliser que les seuls moyens de cryptage** (*) mis à sa disposition par la CUB.
 	
(*) Définition à l'article 10
	- **Utiliser ou détourner à son profit** ou à celui d'un tiers tout ou partie du système d'information auquel il a accès, que ce soit ou non dans l'exercice de ses fonctions.
	- **Porter atteinte**, directement ou indirectement, aux systèmes de traitement automatisés des données, aux bases de données et aux logiciels : intrusion ou utilisation sans autorisation… ; et ce conformément aux dispositions du code pénal.
	- **Intercepter des communications** ou se livrer à la surveillance des autres postes de travail.
	- **Divulguer** des informations nominatives sans le consentement des personnes concernées.

En cas de doute sur la légalité d'une opération, les utilisateurs peuvent consulter les services de documentation qui mettent à leur disposition des ouvrages et textes de lois, ou consulter le code de la propriété intellectuelle sur le site Internet www.legifrance.gouv.fr.

Pour tout conseil juridique, les utilisateurs peuvent s'adresser à la Direction Juridique des Archives et de la Documentation (DIRJAD) ou à la Direction des systèmes d'information (DSI).

5. Bon usage des ressources du système d'information

L'accès aux ressources du système d'information de la CUB n'est possible que dans le **cadre de l'activité professionnelle** des utilisateurs, définie par leur fonction, et dans les limites des **délégations** qui leur sont accordées.

Un usage personnel **ponctuel et raisonnable** des ressources du système d'information (messagerie, Internet, téléphonie, …), dans le cadre des nécessités de la vie courante et familiale, est néanmoins toléré, dans la limite des accès autorisés, dès lors qu'il ne se fait pas au détriment du travail en qualité comme en quantité, et qu'il n'est pas susceptible d'affecter le bon fonctionnement de l'outil informatique ou de mettre en cause l'intérêt et / ou la réputation de la CUB.

Lorsque l'utilisation d'un code identifiant/mot de passe est requis, son utilisation est **strictement personnelle et engage la responsabilité du titulaire du mot de passe**. **Il ne peut en aucune manière être cédé, même temporairement, à un tiers** (y compris un collègue).

Les droits d'accès aux ressources du système d'information nécessitant un code identifiant/mot de passe peuvent être révoqués à tout instant et prennent fin en cas de suspension momentanée ou définitive de l'activité professionnelle (mutation, disponibilité…).

Tout utilisateur est responsable de l'usage des ressources du système d'information auxquelles il a accès. En tant que contributeur clé à la sécurité générale, il doit utiliser ces ressources de **façon rationnelle, loyale et conforme aux obligations légales, professionnelles,** afin d'en éviter la saturation ou le détournement abusif à des fins personnelles.

La protection du **patrimoine informationnel** (*) de la CUB vise avant tout à assurer sa **disponibilité**, son **intégrité** et sa **confidentialité** (communication de l'information aux seules personnes « habilitées à en connaître »). Le rôle de chacun est **fondamental**, dans la mesure où les seules dispositions organisationnelles et techniques prises par la CUB ne sont pas suffisantes.

La DSI, responsable de la sécurité des réseaux, est seule habilitée à diffuser toute information sur les recommandations en matière de sécurité, notamment les virus informatiques. A ce titre la DSI se réserve le droit de supprimer tout élément représentant un risque potentiel.

(*) Définition à l'article 10

L'utilisateur DOIT	L'utilisateur NE DOIT PAS

- **Respecter** les paramétrages des ressources de son poste de travail *notamment ceux relatifs à la sécurité.*
 	
- **Choisir des mots de passe sûrs** et les garder secrets à l'égard de toute personne.
 	
- **Etre vigilant** et **signaler** toute anomalie ou tout constat, tentative ou soupçon de **violation** d'une ressource du système d'information à sa hiérarchie *ou au responsable de la sécurité des systèmes d'information.*
 	
- **Appliquer les recommandations de sécurité** en vigueur dans l'entité à laquelle il appartient.
 	
- **Veiller**, en toutes circonstances, à mettre en sécurité le matériel, notamment micro-ordinateurs portables, assistants personnels, GSM, mis à sa disposition.
 	
- **Observer le respect strict de la confidentialité** nécessaire pour garantir la protection des intérêts de la CUB, des usagers, du personnel, de ses partenaires et de ses prestataires.
 	
- **Veiller** à ce que les informations utiles à son service d'appartenance **soient stockées sur le réseau** dans un répertoire commun**,** pour lequel des dispositions de sécurité et de sauvegarde sont **assurées.**
 	
- **Veiller** à sauvegarder les données locales avec les moyens mis à sa disposition, (CD, clés USB, …).
 	
- **Éviter** en dehors de sa propre activité professionnelle**, tout usage ou toute communication d'information** sur la CUB, les usagers, le personnel les partenaires, et prestataires.
 	
- Veiller à éteindre son poste de travail lors de toute absence prolongée de son lieu de travail
 	
- Limiter au maximum les éditions papier
	- **Introduire** des failles de sécurité dans l'architecture technique du système d'information :
	  - **introduire un élément de connexion à un réseau extérieur (modem, borne WIFI)** sur un micro-ordinateur de la CUB,
	  - **contourner ou désactiver un dispositif de sécurité** protégeant les ressources mises à sa disposition (antivirus du poste de travail, contrôle d'accès à des locaux, …),
	  - **exploiter ni tenter d'exploiter une éventuelle faille de sécurité** du système d'information, ou en faire la publicité.
	
	- **Porter atteinte à l'intégrité du système d'information :**
	  - en perturbant le bon fonctionnement de ce système par son action *(introduction de programmes malveillants tels que virus, bombes logiques, chevaux de Troie…)* ou son inaction,
	  - en dégradant le matériel installé,
	  - en ne modifiant pas la configuration de son poste de travail en installant des périphériques, logiciels, progiciels non agréés par la DSI, *y compris les logiciels libres de droit.*
	
	- **S'approprier ni tenter de s'approprier le mot de passe** d'un autre utilisateur.
	
	- **Utiliser ou essayer d'utiliser des droits** autres que ceux qui lui ont été alloués.
	
	- **Détourner à des fins personnelles ou autres les logiciels** propriété de la CUB ou pour lesquels elle a acquis un droit d'usage.
	
	- **Tenter de lire, modifier, copier ou détruire des données ou documents** autres que ceux dont il a légitimement l'usage.
	
	- **Quitter son poste de travail sans** :
	  - se déconnecter (fermeture des fichiers, applications, sessions en cours) ou verrouiller son micro-ordinateur (mise en veille automatique),
	  - mettre sous clés les documents confidentiels conformément à la charte d'archivage *dès son entrée en vigueur*
	et ce, pour toute absence quelle qu'en soit la durée.

6. Usage de l'Internet et de la messagerie.

La dépendance croissante du système d'information à l'égard des services offerts par INTERNET met en évidence de nouveaux risques auxquels il faut être particulièrement attentif.

De manière préventive, la CUB met en œuvre un certain nombre de dispositifs de filtrage de sites, notamment ceux dont le contenu peut être contraire à l'ordre public, ou aux bonnes mœurs.

Internet est un réseau ouvert et peu sécurisé où la confidentialité des messages n'existe pas. Un acte de piratage est toujours possible.

Internet ne permet pas d'identification fiable de l'expéditeur d'un message, ni de vérification du nom du destinataire. La prudence s'impose.

L'envoi de données confidentielles via le réseau Internet est interdit. En cas d'interception du message par un tiers malveillant, la responsabilité de la CUB serait engagée.

L'utilisation de forums de discussion est autorisée pour un usage exclusivement professionnel, tout utilisateur fait figurer en bas de chacun des messages publiés la mention suivante : « Le contenu de ce message n'engage que son auteur et en aucun cas la CUB »

L'utilisation de services WEBMAIL hébergés de type « Hotmail » est interdite.

L'utilisation des services de messagerie instantanée est interdite aussi bien pour un usage personnel que professionnel.

La diffusion des chaînes et pétitions électroniques est également interdite par l'utilisation de la messagerie de la CUB.

L'utilisateur DOIT	**L'utilisateur NE DOIT PAS**
- **Utiliser** les services Internet dans le cadre strict des droits accordés et des accès autorisés, dans le respect des principes et règles propres aux divers sites concernés. - ***S'assurer qu'il dispose de toutes les autorisations nécessaires*** (licences d'utilisation, droits de reproduction des images, textes et sons) avant d'utiliser ou transférer des données accessibles depuis Internet. - **Faire preuve** de la plus grande correction à l'égard de ses interlocuteurs lors d'échanges électroniques (courrier, forums de discussion …). - **Observer un devoir de réserve** et se garder d'émettre toute opinion susceptible de porter préjudice à l'image de la CUB.	- **Se connecter** ou essayer de se connecter sur un site Internet autrement que par les dispositions prévues par ce site ou sans y être dûment autorisé. - **Consulter ou télécharger** des données (textes, images, sons) ayant un caractère explicitement indécent, contraire à l'ordre public, portant atteinte à la dignité, à la vie privée ou aux droits d'auteur, à caractère injurieux, raciste, pédophile, négationniste, diffamatoire, révisionniste, violent ou en rapport avec une secte , … - De façon dissimulée ou non, **écrire, porter, proférer, transférer ou publier des propos** à caractère injurieux, raciste, pornographique ou diffamatoire. - **Répondre** aux messages « spam » [(*),] **ni cliquer** sur les liens hypertextes insérés dans le corps des spams**.**

(*) définition art. 10

L'utilisateur DOIT	L'utilisateur NE DOIT PAS
- **Signer** ses messages électroniques envoyés à l'extérieur mentionnant, son nom, prénom, qualité, et entité de rattachement, *même si ce message est envoyé depuis une boite aux lettres générique (Boite de Direction).* - **Faire figurer les mentions obligatoires en bas de message, le cas échéant.** - **Traiter le courrier électronique** avec autant de rigueur qu'une véritable correspondance**.** - **Limiter la transmission des fichiers attachés au message électronique** en utilisant soit les répertoires partagés en interne, soit les transferts de fichier en mode Ftp pour l'externe	- **Communiquer** à des tiers des adresses email autres que la sienne sans le consentement des intéressés. - **Envoyer massivement des messages non sollicités** l'utilisateur qui souhaite réaliser un envoi en nombre s'adresse à la DSI qui jugera de l'opportunité d'envoyer un mail en nombre. - **Utiliser la fonction « répondre à tous »** dans le cas des messages envoyés en nombre, en effet ces messages appellent rarement une réponse, le cas échéant l'utilisateur veillera à répondre uniquement à l'auteur du message.

7. Contrôle de l'usage des ressources

Par mesure de sécurité - finalité première -, et pour garantir son utilisation normale, la CUB enregistre les accès ou tentatives d'accès aux ressources de son système d'information.

Le cas échéant, la CUB doit pouvoir :

- identifier et sanctionner les usages abusifs, délictueux ou contraires à ses règles internes en matière de confidentialité et de sécurité,
- répondre aux requêtes émanant des tribunaux ou des organismes de police relatives au comportement de ses utilisateurs, notamment lors de l'usage des ressources de son système d'information.

A ces fins, la CUB met en œuvre des moyens d'enregistrement et d'analyse chaque fois que cela est nécessaire dans le respect de l'information des personnels concernés et des instances représentatives compétentes ainsi que de la législation applicable à l'informatique et aux libertés relative à la protection de la vie privée, de sorte que les informations enregistrées jouissent d'une protection particulière contre tout risque de divulgation.

Lorsque les circonstances l'exigeront (événements menaçant l'intégrité et la sécurité des systèmes d'informations), la CUB pourra être amené à restreindre, voire fermer, sans préavis tout accès aux ressources du système d'information.

Conservation des données :

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.

La CUB a mis en place des procédures pour superviser l'usage des ressources informatiques.

L'objectif est de maintenir la bonne qualité de service en contrôlant le respect des règles de bon usage.

Les abus ont des conséquences négatives pour tous les utilisateurs.

Accès aux traces :

Seuls les administrateurs techniques et les personnels habilités au titre de la sécurité au sein de la DSI et des Directions 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.

Ils ne sauraient non plus être contraints de le faire, sauf disposition législative en ce sens ou une action judiciaire.

Les administrateurs du système habilités à avoir accès aux données de connexion doivent être identifiés.

Usage d'Internet :

Les informations conservées concernant l'utilisation des services WEB sont :

Les sites visités
La durée de connexion au site

Les statistiques mensuelles de l'utilisation d'Internet, diffuées notamment aux Directions, comportent :

- La durée de connexion par Direction, pour chaque utilisateur, sans recoupement avec la liste des sites visités.

Les procédures adoptées pour la messagerie électronique respectent les règles de la correspondance. Elles permettent de conserver les traces d'envoi et de réception des messages.

Usage de la téléphonie (postes fixes comme mobile) :

Les informations suivantes sont conservées :

- la date, l'heure, la durée et le coût de l'appel,
- le numéro du poste appelant,
- le type d'appel (local, national, international, mobile, autres,…),
- le n° appelé.

Ces informations sont comptabilisées à des fins de statistiques mensuelles diffusées notamment aux directions, en masquant les quatre derniers chiffres du n° appelé, conformément à la législation

8. Entrée en vigueur

Cette charte annule et remplace la précédente charte informatique présentée en CTP du 5 mars 2001.

Les utilisateurs sont informés par circulaire de l'existence de la présente charte. Les chefs de service s'assureront de l'affichage de la circulaire et de la remise du document à l'ensemble des utilisateurs placés sous leur responsabilité.

La charte est également disponible sur l'intranet de la CUB et remise à tout nouvel arrivant. Les chefs de service veilleront à une information régulière auprès de leurs agents de son contenu.

9. Modalités d’application

Chaque utilisateur se doit de respecter les dispositions de la présente charte.

Celle-ci sera notamment complétée par une charte spécifique à l’usage du SI pour les agents exerçant un mandat syndical, et par une charte de déontologie pour les administrateurs du SI.

Cette charte doit être annexée à tout contrat de prestation faisant intervenir du personnel ayant accès aux ressources du SI de la CUB.

La DSI met en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.

Le non-respect de la charte peut conduire à une restriction, voire une révocation des droits d’accès au système d’information.

La hiérarchie veille au respect de la présente charte au sein de son service.

Des sanctions disciplinaires peuvent être également instruites, dans le respect des procédures applicables, sans préjuger des éventuelles poursuites judiciaires (pénales ou civiles) qui pourraient être engagées.

Concrètement, en cas de constatation par le chef de service d’un comportement condamné par la présente charte, une procédure disciplinaire peut être engagée à partir de son rapport écrit relatant les faits qu’il transmet à la DRH pour instruction.

10. Lexique et documents de référence

Cryptage : fonctionnalité permettant de transformer des informations confidentielles stockées ou échangées en un contenu inintelligible pour des tiers non habilités à y avoir accès.

Devoir de probité : l'agent public ne doit pas utiliser des moyens de service à des fins personnelles ni avoir d'intérêt dans les personnes morales de droit privé (exemple : entreprise) que ses fonctions l'amènent à contrôler.

Documents de référence : Le rapport de la CNIL relatif à la cyber surveillance sur les lieux de travail (mars 2004)
Le dossier « Relations du travail et internet » issu du forum des droits sur l'internet (26 janvier 2006)

Patrimoine informationnel : qu'il s'agisse d'informations administratives, techniques, financières, il constitue l'un des actifs les plus importants de la CUB sur lequel reposent sa capacité à développer de véritables compétences dans les domaines relevant de ses missions de **service public**, il recouvre :

- Les systèmes d'information nécessaires au plein exercice de ses métiers ;
- Les informations relatives aux usagers ou aux tiers avec lesquels la CUB est en relation, dont l'altération ou la divulgation pourrait porter atteinte à son image de marque, celle des usagers ou des tiers concernés, voire entraîner des poursuites judiciaires ;
- Les informations qu'il incombe à la CUB de conserver en raison d'une obligation *réglementaire, de l'intérêt historique ou technique qu'elles peuvent présenter ;*
- Les informations relatives à ses agents dont la divulgation constituerait une violation de la vie privée.

PSSI : Document de politique stratégique sur la sécurité du système d'information

Ressource du système d'information : l'information et ses différents moyens de partage, de traitement, d'échange et de stockage, l'ensemble étant la propriété de la CUB.

Spam : message commercial envoyé en masse et non sollicité par les destinataires

Système d'information ou SI : **ensemble des moyens humains, techniques et organisationnels** permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et externes de la CUB, **quelle que soit la forme sous laquelle elles sont exploitées** (électronique, imprimée, manuscrite, vocale, image …).

Utilisateur du système d'information : toute personne autorisée à accéder, utiliser ou traiter des ressources du système d'information de la CUB dans le cadre de son activité au sein de la CUB.