ANNEXE

CHARTE INFORMATIQUE

de la Communautē d'agglomēration de Pau Bēarn Pyrēnēes, de la Ville et du CCAS de pau

PAU Capitale humaine

1. PREAMBULE

LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES (ou « collectivité ») met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique ainsi que des outils de mobilité (« Système d'information et de communication »).

Les agents, dans l'exercice de leurs fonctions, et tous autres utilisateurs auxquels l'accès est accordé pour les besoins de leurs fonctions, sont conduits à utiliser le Système d'information et de communication.

La présente charte informatique (la « Charte ») a pour but de promouvoir une utilisation loyale, responsable et sécurisé du Système d'information et de communication dans un cadre de transparence.

Elle a pour objet de définir les conditions de mise à disposition et d'accès à ce système, de préciser ses règles d'utilisation et d'informer des agissements qui peuvent engager la responsabilité des utilisateurs.

Elle définit également les moyens de contrôle et de surveillance de l'utilisation du Système d'information et de communication, non seulement pour la bonne exécution des activités professionnels des utilisateurs, mais aussi dans le cadre de la prévention de la responsabilité de la collectivité.

2. CHAMP D'APPLICATION

2.1 Utilisateurs

Sauf mention contraire, la Charte s'applique à l'ensemble des utilisateurs du Système d'information et de communication, quel que soit leur statut : agents titulaires ; agents contractuels ; intérimaires ; stagiaires ; service civique ; utilisateurs des entités signataires de la convention de service de gestion numérique ; intervenants de sociétés prestataires ; utilisateurs occasionnels (« Utilisateur ») ; etc. Les sociétés prestataires doivent s'engager à faire respecter la Charte par leurs intervenants.

2.2 Système d'information et de communication

Le Système d'information et de communication est constitué de tout système permettant de collecter et/ou de véhiculer l'information adossé à un réseau interne sur lequel les matériels sont connectés.

L'accès et l'utilisation du Système d'information et de communication au travers de matériels personnels connectés à ce système ne seront pas autorisés, sauf autorisation donnée par la Direction du Numérique (DN). Dans cette hypothèse, des logiciels spécifiques pourront être installés par la DN et cette utilisation du Système d'information et de communication sera faite dans le respect de la Charte.

3. REGLES DE SECURITĒ

L'Utilisateur a l'obligation de contribuer à la sécurité générale du Système d'information et de communication. A ce titre, il s'engage à :

• Protéger ses paramètres de connexion (paragraphe 3.1.) ;

• Signaler toute anomalie ou dysfonctionnement à la DN (paragraphe 3.2.) ;

• Respecter les consignes de sécurité (paragraphe 3.3) ;

• Ne pas laisser sans surveillance les visiteurs occasionnels sous sa responsabilité.

3.1 Paramètres de connexion

L'accès au Système d'information et de communication est protégé par des paramètres de connexion (identifiants, mots de passe) qui sont strictement personnels et confidentiels.

L'Utilisateur s'engage à protéger ses paramètres de connexion et notamment à ne pas communiquer ses identifiants et mots de passe à des tiers (dont supérieur hiérarchique), sauf sur demande de la DN. Dans cette dernière hypothèse, si un Utilisateur se trouve dans l'obligation de communiquer ses paramètres de connexion, il procèdera dès que possible au changement de ces derniers ou en demandera la modification à la DN.

Ces paramètres de connexion doivent être mémorisés par l'Utilisateur (et/ou stockés dans un système de coffre-fort électronique archivant les mots de passe) et ne pas être reproduits sur un support quelconque.

L'utilisateur suit les préconisations en ce qui concerne la robustesse de ses mots de passe. Les paramètres de connexion doivent être modifiés selon une fréquence déterminée par la DN.

Il est recommandé d'avoir des mots de passes différents en cas de connexions à des applications/logiciels multiples. Il est impératif de distinguer les mots de passe professionnels des mots de passe personnels.

Enfin, aucun mot de passe professionnel ne doit être utilisé pour des comptes personnels.

3.2 Informations

L'Utilisateur s'engage à signaler à la DN toute anomalie, problème technique, tentative d'intrusion, tentative de phishing, faille de sécurité, perte de ses paramètres de connexion ou toute autre difficulté de ce type, et à prendre toutes les mesures de sauvegarde de ses données et fichiers professionnels sur tout support proposé par la DN.

Par ailleurs, l'Utilisateur signale à son supérieur hiérarchique toute divulgation d'informations confidentielles ou susceptibles de porter atteinte à l'image de son employeur. Pour les données à caractère personnel, se référer au chapitre TRAITEMENT DES DONNEES A CARACTERE PERSONNEL.

3.3 Consignes de sécurité

L'Utilisateur n'est pas autorisé à modifier les paramètres et désinstaller les outils de sécurité installés par la DN. En outre, l'Utilisateur s'engage à ne pas laisser à la portée de tous les matériels et supports informatiques mis à sa disposition, à verrouiller sa session informatique en son absence et à ne pas utiliser la session d'un autre Utilisateur. Par ailleurs, l'Utilisateur :

• N'utilise pas le Système d'information et de communication pour proposer ou rendre accessibles à des tiers des données et informations confidentielles conformément à l'article « Confidentialité » de la Charte ;

• S'engage à ne pas désinstaller des logiciels ou progiciels et particulièrement les outils de sécurité mis en place par la DN ;

• N'apporte volontairement pas de perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus et chevaux de Troie, notamment).

LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES pourra, de manière unilatérale, désinstaller tout dispositif qui nuirait à la sécurité du Système d'Informations ou à la protection des données.

Dans le cadre de l'utilisation d'Internet, l'Utilisateur s'engage à faire preuve de vigilance en cas de suspicion de méthodes frauduleuses telles que le phishing (tentative d'acquérir des informations confidentielles - identifiants, mots de passe, cryptogrammes – en usurpant l'identité d'un tiers digne de confiance).

Dans le cadre de l'utilisation de sa messagerie électronique, avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations, liens et pièces jointes transmises. L'Utilisateur s'engage à choisir précisément les destinataires principaux et ceux en copie des messages électroniques, à porter une attention particulière à l'utilisation des fonctions « répondre à tous » ou « répondre à tous avec historique », et à utiliser un logiciel de compression avant tout envoi de fichiers volumineux. L'utilisateur doit également envisager l'opportunité de dissimuler certains destinataires,

en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

4. CONDITIONS D'UTILISATION DU SYSTEME D'INFORMATION ET DE COMMUNICATION

L'Utilisateur s'engage à ne pas faire un usage du Système d'information et de communication susceptible de nuire ou de porter atteinte aux droits et intérêts d'un tiers physique ou moral.

Il s'engage en conséquence à :

• Respecter les règles d'utilisation, limites et interdictions posées par la Charte.

• Utiliser les outils informatiques et de communication mis à sa disposition conformément aux instructions qui lui auront été données par son supérieur hiérarchique et/ou par la DN.

• Rendre le jour de son départ, tout matériel professionnel appartenant à LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES mentionné dans la fiche de remise de matériel et s'assurer que les dossiers, les fichiers et les messages professionnels sont intègres, accessibles et lisibles (clés de cryptage ou mot de passe éventuels fournis à la DN).

4.1 Utilisation d'Internet

Dans le cadre de leur activité, les Utilisateurs ont accès à Internet. Pour des raisons de sécurité et de qualité du Système d'information et de communication, la collectivité informe les Utilisateurs que :

• Leur navigation sur Internet, via le Système d'information et de communication, est filtrée et enregistrée.

• L'accès à certains sites peut être limité ou prohibé. La collectivité peut imposer des configurations du navigateur et installer des mécanismes de filtrage limitant leur accès.

Par ailleurs, la collectivité interdit à l'Utilisateur, d'accéder à des fins personnelles, à des sites d'enchères en ligne et de commerce électronique, de procéder à des opérations boursières en ligne, de participer à des jeux de hasard, d'argent et de paris sportifs en ligne, à des jeux en réseau, d'accéder à des sites à caractère pornographique ou dont l'accès aux mineurs est interdit ou à tout site non approprié.

L'Utilisateur ne doit pas accéder à des sites permettant le téléchargement illégal (Ex. : peer-to-peer) ou la visualisation d'œuvres sans droit (Ex. streaming).

La collectivité se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité ou altérer le bon fonctionnement du Système d'information et de communication.

4.2 Utilisation de la messagerie électronique

Les utilisateurs disposent, pour l'exercice de leur activité professionnel, d'une adresse de messagerie électronique normalisée attribuée par la DN.

Il n'est pas permis de faire usage de sa messagerie professionnelle à des fins promotionnelles, de mettre en place un système de transfert automatique de courriers électroniques reçus sur la messagerie électronique professionnelle vers un ou plusieurs comptes de messagerie électronique n'appartenant pas à LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES et de se livrer à des actes d'envoi massif de courriers électroniques non sollicités (spamming).

4.3 Utilisation à des fins personnelles

Le Système d'information et de communication est mis à la disposition dans le cadre de l'exercice de son activité professionnelle. Chaque Utilisateur est responsable du bon usage de ce système et des données auxquelles il accède.

Un usage raisonnable du Système d'information et de communication à des fins personnelles est toutefois autorisé, à condition de respecter la loi en vigueur et les règles de la Charte. Dans cette hypothèse, l'Utilisateur devra identifier comme personnel tout fichier ainsi que tout courrier électronique enregistrés sur le Système d'information et de communication. Ces fichiers et courriers électroniques doivent être signalés par la mention « PERSONNEL » dans leur objet et/ou dans leur titre ou être classés dans un dossier lui-même portant la mention « PERSONNEL ». A défaut, le fichier ou le courrier électronique sera présumé être à caractère professionnel.

L'utilisation à titre personnel du Système d'information et de communication ne doit en aucun cas :

• Gêner le trafic normal des échanges professionnels.

• Perturber le bon fonctionnement du réseau.

• Réduire la productivité et la qualité du travail de l'Utilisateur.

En outre, l'Utilisateur ne pourra en aucun cas engager la responsabilité de LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES dans l'hypothèse dès lors qu'un contenu personnel serait accidentellement détruit, ou subirait des altérations du fait de tiers.

Par ailleurs, l'Utilisateur s'engage, au plus tard le jour de son départ effectif, à retirer et/ou détruire lui-même tous les fichiers et messages identifiés comme personnels lui appartenant qu'il aurait stockés sur le Système d'information et de communication.

A défaut, la collectivité pourra dès le départ effectif de l'Utilisateur procéder à cette suppression et l'Utilisateur ne pourra en aucun cas se retourner contre elle.

Enfin, l'Utilisateur ne doit pas conserver postérieurement à son départ effectif tout contenu appartenant à son employeur. Il pourra cependant, en cas de procédure contentieuse avec elle, prendre avec lui les mails et documents pouvant assurer sa défense en cas de départ.

4.4 Utilisation des logiciels

Tout téléchargement, installation et utilisation de logiciels est soumis au contrôle et à l'autorisation préalable de la DN.

Le matériel mis à disposition ne doit pas contenir de programmes, logiciels, documents, fichiers, informations ou données contrevenant d'une façon ou d'une autre à la loi ou à la Charte et peuvent faire l'objet de vérifications et de contrôles par la DN dans les limites prévues par la loi.

Il n'est pas permis de vendre ou de transférer des logiciels, de la documentation ou tout autre type d'informations ou données internes à un tiers, sauf accord préalable et écrit de son employeur.

Les échanges d'informations, de logiciels et/ou de données entre LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES et une tierce partie ne peuvent avoir lieu, sauf dans le cas où un contrat approprié a été préalablement signé.

En outre, l'Utilisateur ne doit pas procéder à des copies de logiciels fournis dans le cadre de son activité professionnelle.

4.5 Utilisation des médias sociaux

Les Utilisateurs doivent utiliser les médias sociaux de façon responsable et respectueuse du Règlement Intérieur en se conformant au code général de la Fonction Publique portant droits et obligations des fonctionnaires.

Lors de la création de son compte personnel à usage professionnel, il est recommandé à l'Utilisateur d'utiliser une adresse électronique personnelle, avec un mot de passe fortement éloigné de celui utilisé dans le cadre professionnel, afin de ne pas compromettre un accès direct à sa messagerie professionnelle.

4.6 Contenus illicites

Il est interdit à l'Utilisateur de solliciter l'envoi par des tiers, de télécharger, de stocker et/ou diffuser à partir du Système d'information et de communication, tout contenu contraire à l'ordre public et aux bonnes mœurs, présentant un caractère injurieux ou diffamatoire au sens de l'article 29 de la Loi du 29 juillet 1881 ; portant atteinte aux droits des personnes et des biens, et notamment au droit à l'image et à la vie privée des personnes tels que visés à l'article 9 du Code civil, ou susceptible de porter atteinte à la présomption d'innocence visée à l'article 9-1 du Code civil.

Il est également expressément interdit à l'Utilisateur de télécharger, stocker et/ou diffuser à partir du Système d'information et de communication, ou solliciter l'envoi par des tiers de tout information, texte, image (animée ou non), donnée, son, fichier multimédia, hyperlien violant ou méconnaissant les droits de propriété intellectuelle de quelque tiers que ce soit ou permettant ou facilitant la réalisation d'actes de contrefaçon.

Cet engagement porte également sur tout contenu constitutif de délits, ou incitant à la discrimination raciale, la xénophobie, l'homophobie, révisionnisme, la haine ou la violence à l'égard d'une personne ou d'un groupe en raison de son origine, de son appartenance ou de sa non appartenance à une ethnie, une nation, une race ou une religion déterminée, présentant une menace à l'égard d'une personne ou d'un groupe de personnes, incitant à la commission d'un délit, d'un crime ou d'un acte de terrorisme, faisant l'apologie des crimes de guerre ou des crimes contre l'humanité ou constituant une provocation au suicide.

Il est enfin interdit à l'Utilisateur d'utiliser l'un des éléments du Système d'information et de communication pour réaliser tout acte constitutif des délits d'atteintes aux traitements automatisés de données prévus et réprimés par les articles 323-1 et suivants du Code pénal.

4.7 Conditions d'accès aux ressources

Tout Utilisateur doit s'organiser pour que l'ensemble des informations liées à son travail soit accessible par son supérieur hiérarchique.

Chaque Utilisateur doit veiller à recourir aux espaces collaboratifs utilisés par son service pour veiller à la poursuite de l'activité lors d'une absence ponctuelle (Ex. : en raison d'un congé ou d'un arrêt maladie). L'Utilisateur ne doit pas transmettre son mot de passe à son responsable hiérarchique.

Si l'accès s'avère nécessaire à la poursuite de l'activité, le chef de service ou directeur pourra (selon les modalités déterminées par la Direction du Numérique) accéder aux informations contenues dans les équipements utilisés par l'Utilisateur. Dans ce cas, le chef de service ou directeur fera une demande d'accès justifiée auprès de la DN. L'Utilisateur concerné sera informé de cet accès (hors départ définitif). Dans le cadre d'une demande d'accès jugée complexe ou sensible, l'avis du DPO sera sollicité. Dans tous les cas, cet accès sera réalisé dans les conditions propres à garantir le droit au respect de la vie privée de l'Utilisateur (pas de consultation/extraction d'éléments mentionnées « personnel »).

La Direction du Numérique pourra créer un message d'absence si cela s'avère nécessaire. Cela permettra de limiter la nécessité d'accéder aux ressources de l'agent.

Par ailleurs et conformément à la jurisprudence de la Cour de cassation, l'employeur pourra si nécessaire accéder aux fichiers et courriers électroniques personnels de l'Utilisateur après avoir obtenu l'autorisation de la juridiction compétente à cette fin.

4.8 Contrôle du système d'information et de communication

Pour assurer la sécurité du Système d'information et de communication, l'Utilisateur est informé que la DN peut procéder au contrôle de toute application, fichier ou message électronique à l'exception de ceux identifiés comme étant personnels.

La DN peut ainsi intercepter ou bloquer tout flux informatique présentant des risques pour la sécurité et/ou la qualité du Système d'information et de communication, vérifier de manière automatisée la conformité de sécurité d'un matériel avant son accès au réseau informatique interne, explorer les fichiers et messages électroniques professionnels des Utilisateurs en cas de suspicion ou de constat d'actes d'atteinte au système de traitement automatisé de données, supprimer et interdire des applications en cas de risques pour la sécurité du SI.

Elle peut également contrôler et enregistrer les flux de chaque Utilisateur afin de prévenir la propagation de virus, contrôler ponctuellement les sites visités par chaque Utilisateur, vérifier le contenu des données et documents stockés sur chaque ordinateur à l'exception de ceux désignés comme étant personnels.

Par défaut, la DN n'a pas accès à la position des téléphones. Les données de géolocalisation des téléphones ne sont activées que si l'utilisateur a activé par lui-même la localisation. Cette donnée ne sera utilisée que dans le cadre de la recherche d'un matériel perdu ou volé à la condition que l'Utilisateur ait activé par lui-même la fonction au préalable.

La DN peut contrôler, et éventuellement supprimer les courriers électroniques envoyés et/ou reçus par chaque Utilisateur, fichiers et tout support informatique sans que l'accord de l'Utilisateur soit recherché, dès lors que le contenu ne porte pas la mention « PERSONNEL ».

La suppression des courriers électroniques, fichiers ou support informatique aura lieu après information par LA COMMUNAUTÉ D'AGGLOMÉRATION PAU BÉARN PYRÉNÉES de l'utilisateur concerné. En revanche, en cas de risque immédiat pour la sécurité du SI, cette suppression peut avoir lieu sans préavis par les équipes techniques.

5. TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Le règlement général sur la protection des données (RGPD) définit les conditions dans lesquelles les traitements de données à caractère personnel peuvent être effectués. La Communauté d'Agglomération Pau Béarn Pyrénées a désigné un délégué à la protection des données (DPO). Ce dernier a pour mission de veiller au respect de ce règlement.

Aussi, tout utilisateur amené à effectuer une opération portant sur des données à caractère personnel doit tenir informé le DPO de sa collectivité, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes concernées et les mesures de sécurité à déployer pour protéger les données.

Chaque utilisateur s'engage à stocker les données à caractère personnel dans l'espace de stockage approprié en fonction de la sensibilité et/ou la confidentialité requises (dossier avec accès restreint et sécurisé, équipe privée, espace de stockage individuel, Hébergement Données de Santé, etc.) et à classifier l'information (public, privé, confidentiel) selon les outils et modalités préconisées par la DN et le DPO.

Tout utilisateur subissant une violation de données à caractère personnel (incident de sécurité ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles) devra en informer le DPO afin que celui-ci enclenche les démarches nécessaires.

Le DPO veille également au respect des droits des personnes (droit d'accès, de rectification et d'opposition, effacement, limitation). Consultez le site cnil.fr pour plus d'informations sur vos droits.

Coordonnées du DPO :

- Communauté d'Agglomération Pau Béarn Pyrénées : dpo@agglo-pau.fr
- Ville de Pau : dpo@ville-pau.fr
- CCAS : dpo@ccas-pau.fr

5.1 Information des utilisateurs

La Charte est annexée au Règlement Intérieur. En application du Règlement Intérieur, le non-respect de la Charte peut entrainer une sanction disciplinaire.

Pour les agents nouvellement recrutés, la charte leur est communiquée lors de leur arrivée.

Pour les agents en fonction avant l'entrée en vigueur de la Charte, elle leur est communiquée individuellement par courrier électronique ou à la première connexion depuis la validation du Règlement Intérieur. Elle pourra aussi être imprimée par les encadrants lorsque cela est nécessaire.

5.2 Travail en mobilité

L'utilisation d'équipements personnels, même pour des usages en mobilité, n'est pas autorisée.

L'Utilisateur doit prévenir la DN de ses déplacements à l'étranger afin d'étudier les modalités d'accès au Système d'Information et de communication. Aucune étude ne sera réalisée pour des déplacements à titre personnels.

En situation de mobilité, l'ensemble de la présente charte s'applique y compris la confidentialité de la collectivité. Cela comprend la protection de toutes les informations confidentielles auxquelles vous pouvez accéder, et la sauvegarde régulière des données importantes. Vous devez également prendre les mesures nécessaires pour : garantir la sécurité de votre environnement de travail en mobilité ; vous assurer que des tiers n'ont pas accès aux équipements et aux données de l'entreprise ; verrouiller l'accès de votre matériel informatique afin de s'assurer d'en être le seul utilisateur ; utiliser le VPN pour accéder au système d'informations.

QUESTIONS

Chaque Utilisateur peut s'adresser à la DN pour toute question concernant l'application de la Charte, laquelle la soumettra si besoin à la Direction appropriée pour y répondre.