HAUTE-CORRÈZE COMMUNAUTÉ

2019

Ressources Informatiques

CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES FOURNIES PAR HAUTE CORREZE COMMUNAUTE

MARC ANTOINE SALLAS

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

PREAMBULE

Haute Corrèze Communauté met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de Haute Corrèze Communauté.

Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de la collectivité.

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

CHAMP D'APPLICATION

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de Haute Corrèze Communauté pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils n'est pas tolérée. La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur le serveur.

Elle est systématiquement remise à tout nouvel arrivant. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Les agents veillent à faire accepter valablement les règles passées dans la présente charte a toute personne à laquelle ils permettraient d'accéder au système d'information.

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail de salariés.

Quelques définitions :

Utilisateur

On désignera sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de Haute Corrèze Communauté et à les utiliser : employés, stagiaires, partenaires, prestataires, visiteurs occasionnels....

Outils informatiques et de communication

Les termes "outils informatiques et de communication" recouvrent tous les équipements informatiques, de télécommunications et de reprographie de Haute Corrèze Communauté.

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par Haute Corrèze Communauté.

Les modalités d'intervention du service « Système d'Information » (SI)

Le service « Système d'Information » assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de Haute Corrèze Communauté. Les agents de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée à Haute Corrèze Communauté. Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels. Actuellement, le mot de passe doit être composé de 7 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement : tous les 3 mois.

Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

Signaler au service SI de Haute Corrèze Communauté toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.

- Ne jamais confier son identifiant/mot de passe.

- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de Haute Corrèze Communauté.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par Haute Corrèze Communauté.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de Haute Corrèze Communauté sans l'accord préalable du service SI. Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes.

Dès lors, les contrats signés entre Haute Corrèze Communauté et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

LES MOYENS INFORMATIQUES

Configuration du poste de travail

Haute Corrèze Communauté met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par le service SI.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement dit nomade »)
- Nuire au fonctionnement des outils informatiques et de communications. Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du service SI.

Équipements nomades et procédures spécifiques aux matériels de prêt

Équipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc.…).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par le service SI, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (exemple : vidéoprojecteur). Il en assure la garde et la responsabilité et

doit informer le service Système d'Information en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

Internet

Accès aux sites

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par le service système d'information qui est habilité à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite.

Il est aussi prohibé de créer ou mettre à jour au moyen de l'infrastructure de la collectivité tout site Internet, notamment des pages personnelles. Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de la collectivité ou engageant financièrement celle-ci.

Autres utilisations

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer la direction informatique.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de la collectivité.

Ils sont informés que le service Système d'Information enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'entreprise.

Messagerie électronique

Des agents disposent, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par le service Système d'Information.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service Système d'Information, et validées par celui-ci :

- volumétrie de la messagerie,

- taille maximale de l'envoi et de la réception d'un message,
- nombre limité de destinataires simultanés lors de l'envoi d'un message,
- gestion de l'archivage de la messagerie.

En cas de nécessité de service, le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les agents peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (webmail) et sur leur téléphone professionnel. Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier postal : il obéit donc aux mêmes règles, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de la collectivité et de l'utilisateur.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par le service Système d'information.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il 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. En cas d'envoi à une liste de diffusion, il est important d'en vérifier les modalités d'abonnement, de contrôler la liste des abonnés et de prévoir l'accessibilité aux archives. Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.

Ils doivent, le cas échéant, être doublés par un envoi de fax ou de courrier postal.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par le service Système d'Information, pour ce qui concerne la mise en forme et surtout la signature des messages.

En cas d'absence supérieure à 3 jours, le salarié doit mettre en place un répondeur automatique.

Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par le service Système d'Information. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au service Système d'Information, qui est aussi chargée de l'ouverture des listes de diffusion qui pourraient s'avérer nécessaires.

De même, le service Système d'Information peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale d'un an. Passé ce délai, ils sont automatiquement supprimés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide du service Système d'Information si nécessaire. Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles.

Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention

"Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso".

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Utilisation de la messagerie par la délégation du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la

même manière que les messages à caractère personnel, mais en utilisant la mention "Délégué" dans leur objet à l'émission et dans le dossier où ils doivent être classés

Consultation de la messagerie

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, le service Système d'Information de Haute Corrèze Communauté peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation). Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés. En cas d'absence prolongée d'un agent (longue maladie par exemple), le chef de service peut demander au service SI, après accord de son directeur, le transfert des messages reçus.

Courriel non sollicité

Haute Corrèze Communauté dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion.

Téléphone

Haute Corrèze Communauté met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone mis à disposition par Haute Corrèze Communauté est seulement à usage professionnel. Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. À titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Haute Corrèze Communauté s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

Haute Corrèze Communauté s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le SI, sur demande (nom de la personne compétente. Ex : DGS, DGA…) se réserve le droit d'accéder aux numéros complets des relevés individuels.

L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du Système d'Information de Haute Corrèze Communauté, différents dispositifs sont mis en place.

Les systèmes automatiques de filtrage

À titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour Haute Corrèze Communauté et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée…).

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

Les systèmes automatiques de traçabilité et contrôle des activités

Contrôles automatisés

Le service Système d'Information s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau.

Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de la collectivité, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers ;
- aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable au service Système d'Information. De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 30 jours après leur enregistrement.

Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service Système d'Information, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de la

collectivité, ou sur sa messagerie. Alors, sauf risque ou événement particulier, le service Système d'Information ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

Gestion du poste de travail

À des fins de maintenance informatique, le service Système d'Information de Haute Corrèze Communauté peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur. Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service Système d'Information peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer au service Système d'Information les matériels mis à sa disposition.

Toute copie de documents professionnels n'est pas autorisée.

Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

Informations et Sanctions

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre émanant du service Système d'Information, après avis du Directeur General Adjoint du Service Ressources, en cas de non-respect des règles énoncées par la charte ;
- dans un second temps, et en cas de renouvellement, après avis du Directeur General Adjoint du Service Ressources, et du supérieur hiérarchique de l'agent, en des sanctions disciplinaires.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

Envoyé en préfecture le 01/10/2019
Reçu en préfecture le 01/10/2019
Affiché le
ID : 019-200066744-20190926-2019030323-DE

Entrée en vigueur de la Charte

La présente charte a été adoptée après information et consultation du comité technique et du conseil communautaire.

Elle est applicable à compter du …….

ANNEXE

Disposition légales applicables

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

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.

Dispositions Pénales :

- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels. Disposition pénale : art L.335-2 du Code pénal.