Conseil départemental

Haut-Rhin

Charte d'utilisation des ressources T.I.C.

	Entité	Nom	Fonction	Date
Rédacteur	CD68/DSI	A.KASPER	Chargée de mission affaires juridiques et marchés publics	17/07/2017
Approbateurs	CD68/DSI	R.NATTER	Directeur	
	CD68/DGA	S.TACHON	Directeur Général Adjoint	
	CD68/DGS	P.JAMET	Directeur Général des Services	
	CTP	CTP		05/10/2017
Responsable du document	CD68	A.KASPER	Chargée de mission affaires juridiques et marchés publics	

HISTORIQUE DES REVISIONS DU DOCUMENT

VERSION	DATE	MODIFICATIONS	AUTEUR(S)
1	17/07/2017	Document initiale (V0)	A.KASPER
2	04/09/2017	Validation en CSDSI (V1)	A.KASPER
3	05/09/2017	Insertion modifications DJU et DRH (V2)	A.KASPER

SOMMAIRE

1 Préambule

La présente charte a pour objet de définir les règles d'utilisation des ressources en matière de technologies de l'information et de la communication (T.I.C.) tant pour les utilisateurs que pour la collectivité.

Ces règles doivent permettre d'obtenir un usage normal, optimal et sécurisé des ressources T.I.C. du Département du Haut-Rhin. Elles ont 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.

Cette charte s'applique à toute personne utilisatrice des ressources T.I.C. du Département du Haut-Rhin.

On désigne sous le terme « utilisateur » toute personne (Conseiller départemental, agent, prestataire externe, partenaire, stagiaire, …) ayant accès ou utilisant les ressources T.I.C. mises à disposition par le Département.

On désigne de façon générale sous le terme de « ressources T.I.C. » :

- les outils informatiques (PC fixes, PC portables, logiciels, accessoires…)
- les outils de communications (télécopieurs, téléphones fixes, téléphones mobiles…)
- les services Internet (messagerie, Intranet, Extranet, Internet…)

Les règles fixées dans la présente charte, dont le respect conditionne le droit d'accès aux ressources T.I.C., sont applicables à l'ensemble des utilisateurs du Département et leur sont opposables de plein droit.

L'adhésion de chaque utilisateur emporte la mise en jeu de sa responsabilité par :

- Un engagement à utiliser de manière raisonnable et raisonnée les ressources mises à sa disposition ;
- Un engagement à respecter la réglementation applicable.

La violation des règles fixées dans la présente charte peut donner lieu, selon les utilisateurs, à l'application d'une sanction disciplinaire, indépendamment d'éventuelles poursuites pénales et/ou civiles.

2 Champ d'application de la Charte

2.1 Conditions d'accès

L'accès aux ressources T.I.C. du Département est destiné à un usage professionnel conformément à la législation en vigueur.

Il est demandé (cf. article 2.7) de ne pas quitter son poste de travail sans le verrouiller ou l'éteindre afin de ne pas laisser des ressources disponibles sans identification.

L'utilisateur est responsable de l'usage des ressources locales ou distantes mises à disposition à partir de ses droits d'accès.

Les codes d'accès attribués à l'utilisateur, par le Département, en fonction de ses missions, sont strictement personnels et incessibles.

Ils sont également temporaires. Ils peuvent être retirés notamment dans les cas suivants :

- lors du départ de l'utilisateur,
- lorsque sa fonction ne le justifie plus,
- en cas de non-respect de la présente charte.

Lorsque l'accès à un service requiert l'ouverture d'un compte nominatif, l'utilisateur doit s'en servir, à l'exclusion de tout autre. Il peut lui être demandé de saisir et de changer régulièrement de mot de passe.

Toutes les connexions réalisées à l'aide des codes d'accès de l'utilisateur engagent la responsabilité de ce dernier dans les conditions définies dans la présente charte.

2.2 Les principes généraux d'utilisation des ressources

Retrouver les guides pratiques sur le portail des services informatiques (Intranet)

Le Département par l'intermédiaire de la Direction des Systèmes d'Information, gestionnaire des ressources T.I.C., met à disposition des utilisateurs de son réseau les ressources informatiques et téléphoniques nécessaires au bon déroulement de leurs missions et assure l'information nécessaire à leur correcte utilisation.

L'usage des ressources est réservé à l'activité professionnelle liée à l'exercice des missions du Département du Haut-Rhin. L'utilisation des ressources à titre privé ne peut constituer qu'une simple tolérance (utilisation occasionnelle et raisonnée) tant qu'elle ne porte pas atteinte à l'exercice de la mission de service public et qu'elle n'affecte pas la sécurité et la productivité des systèmes d'information.
Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources T.I.C., ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi informatique et libertés et du règlement général sur la protection des données.

Les utilisateurs s'engagent à respecter la présente charte et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- De masquer leur véritable identité ;
- D'usurper l'identité d'autrui ;
- D'obtenir le mot de passe d'un autre utilisateur ;
- D'altérer les données ou d'accéder à des informations appartenant à d'autres utilisateurs, sans leur autorisation ;
- De modifier ou de détruire des ressources connectées au réseau ;
- D'interrompre même temporairement, le fonctionnement normal du réseau ou de l'un des systèmes connectés au réseau ;
- De modifier le fonctionnement, le paramétrage et les caractéristiques du poste de travail mis à disposition.

2.3 Le matériel

Les utilisateurs se voient doter, selon les indications de l'autorité hiérarchique, par la Direction des Systèmes d'Information, de ressources T.I.C. nécessaires à l'exercice de leurs missions.
Ces ressources sont intégrées dans l'annuaire informatique permettant de référencer les matériels affectés et de définir les autorisations d'accès aux applications et aux réseaux.

Dans tous les cas, l'utilisateur est responsable du matériel qui lui a été confié.

- En cas de perte de matériel, l'utilisateur devra avertir sans délai la Direction des Systèmes d'Information, par note sous couvert de son supérieur hiérarchique.
- En cas de vol de matériel, l'utilisateur devra sans délai aller effectuer un dépôt de plainte auprès des autorités compétentes (gendarmerie ou police) et avertir la Direction des Systèmes d'Information, par note sous couvert de son supérieur hiérarchique en y annexant la copie du dépôt de plainte.

L'utilisateur ne doit pas modifier sa configuration, ni procéder à des ajouts de périphériques. En cas de besoin, il peut demander par voie hiérarchique à la Direction des Systèmes d'Information d'être doté de matériel supplémentaire.

Les équipements non fournis par le Département (ordinateurs portables, smartphones, …) ne peuvent être connectés aux systèmes d'information sans l'accord préalable de la Direction des Systèmes d'Information.

Les supports numériques (clé USB, CD, DVD, disque dur externe…) sont mis à disposition à des fins strictement professionnelles. Aucune utilisation à des fins privées n'est autorisée.

Equipements nomades :

On entend par équipements nomades, tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphone mobile ou smartphone, clé USB, etc.).

L'utilisation de smartphone 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.

2.4 Les logiciels

Chaque utilisateur est doté de logiciels adaptés à ses missions.
Il ne doit pas, sans autorisation de la Direction des Systèmes d'Information, équiper son poste de logiciels supplémentaires. Il lui est formellement interdit de copier les logiciels d'autres utilisateurs et d'utiliser des logiciels dont le Département n'aurait pas acquis les licences.

2.5 Propriété intellectuelle

Les ressources T.I.C. ne doivent en aucune manière être utilisées à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits

prévus aux livres Ier et II du code de la propriété intellectuelle lorsque cette autorisation est requise.
L'utilisateur est tenu de se conformer à la politique de sécurité du Département, y compris aux règles d'utilisation des moyens de sécurisation (politique antivirale, gestion mot de passe, sauvegarde, …) mises en œuvre dans le but de prévenir l'utilisation illicite des ressources T.I.C. et de s'abstenir de tout acte portant atteinte à l'efficacité de ces moyens.

Infraction punie d'une peine d'amende d'un montant maximum de 7500 euros pour les personnes morales, qui peut être assortie d'une peine de suspension de l'accès à internet d'une durée maximum d'un mois.

Il est rappelé à cet égard que le Département en tant que titulaire d'un accès à Internet est tenu de sécuriser cet accès afin qu'il ne soit pas utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin. S'il ne se conforme pas à cette obligation, le titulaire peut voir sa responsabilité pénale engagée au titre de la négligence caractérisée (article R.335-5 du code de la propriété intellectuelle).

Cette responsabilité du titulaire de l'accès n'exclut en rien celle de l'utilisateur qui peut se voir reprocher un délit de contrefaçon (article L. 335-3 du code de la propriété intellectuelle).

2.6 Les fichiers

L'ensemble des données saisies et mises en forme par l'utilisateur dans le cadre de ses missions sont par défaut des données professionnelles.

La sauvegarde des données stockées sur les espaces de stockage partagé est assurée par les administrateurs de la Direction des Systèmes d'Information des systèmes d'Information.

Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires explicitement prévus à cet effet et intitulés « privé » ou « personnel ».

La protection et la sauvegarde régulière des données de ces dossiers incombent à l'utilisateur, la responsabilité du Département ne pouvant être engagée quant à la conservation de cet espace.

Par ailleurs, il est interdit d'utiliser des données contenues dans les fichiers du Département pour une finalité différente que celle pour laquelle elles ont été collectées et ce même si ces données ne seraient pas explicitement protégées.

2.7 Règles de sécurité

La protection des données face aux menaces de perte, vol ou modification ne peut être garantie par la seule action de la DSI, mais l'action conjuguée de tous

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

- Signaler à la Direction des Systèmes d'Information 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 du Département.
- Verrouiller ou éteindre 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 le Département.

En outre, il convient de rappeler que toute personne qui n'est pas utilisateur des ressources T.I.C. au sens de la présente Charte (visiteurs notamment) ne peut avoir accès au Système d'Information du Département sans l'accord préalable de la Direction des Systèmes d'Information.

Les prestataires externes doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre le Département et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

2.8 Protection des données à caractère personnel

Avant de créer un fichier contenant des données personnelles, l'utilisateur est tenu de consulter le délégué à la protection des données personnelles qui vérifiera la conformité du fichier aux dispositions en vigueur en matière de protection des données à caractère personnel.

Le délégué à la protection des données personnelles est joignable par mail (dpd@haut-rhin.fr).

Ce dernier pourra le conseiller et lui indiquer les éventuelles obligations à respecter, notamment en matière d'information des personnes concernées par les données. En effet, les personnes concernées par un traitement de données à caractère personnel doivent être informées des finalités et de la destination des informations enregistrées, de la durée de conservation (nécessaire à la réalisation de la finalité du traitement) ainsi que de leur droit d'accès, modification et de rectification des données les concernant.

De plus, il est rappelé qu'aucune information concernant les croyances, idéologies, appartenances politiques, mœurs sexuelles, appartenances raciales ou éthiques ne peut être collectée.

Par ailleurs, chaque utilisateur dispose d'un droit d'accès, de modification et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.

2.9 Utilisation d'Internet

Pour des besoins de sécurité, les traces des sites consultés par les utilisateurs sont conservées pendant un an conformément à la législation en vigueur (art. R10-12 à R.10-14 du code des postes et des communications électroniques)

L'utilisation d'internet constitue un élément essentiel d'accessibilité de l'information.

Seuls ont vocation à être consultés les sites internet présentant un lien avec l'activité professionnelle.

Le Département du Haut-Rhin tolère, conformément aux recommandations de la Commission Nationale de l'Informatique et Libertés (C.N.I.L.), une consultation ponctuelle et dans des limites raisonnables, pour un motif personnel, de sites Internet dont le contenu n'est pas contraire à l'ordre public ni aux bonnes mœurs et ne met pas en cause l'intérêt et la réputation de la collectivité, ni la sécurité et la productivité des systèmes d'information.

Il est interdit d'effectuer des achats ainsi que des téléchargements de logiciels ou d'autres œuvres protégées sauf dérogation expresse de la Direction des Systèmes d'Information accordée au regard des missions de l'utilisateur.

La Direction des Systèmes d'Information met en œuvre un système de contrôle permettant de bloquer l'accès à certains sites considérés comme dangereux pour le système informatique ou illégaux aux regards de leurs contenus présumés.

2.10 Utilisation de la messagerie

Il convient de limiter la diffusion de son adresse e-mail professionnelle sur Internet.

Le risque de recevoir des messages indésirables « spamming » est important et cela encombre la messagerie

Le système de courrier électronique est réservé à une utilisation professionnelle permettant à chaque utilisateur de communiquer en interne et en externe.

Le Département du Haut-Rhin, conformément aux recommandations de la Commission Nationale de l'Informatique et Libertés (C.N.I.L.), admet un usage raisonnable, dans le cadre de la vie courante des messages personnels dans la mesure où ceux-ci n'affectent pas le trafic normal des messages professionnels.

En l'absence de toute indication contraire (mention « privé » ou « personnel »), un message électronique est considéré comme un message professionnel et non comme un message personnel.

Le Département du Haut-Rhin s'interdit d'accéder aux dossiers et aux messages identifiés comme « privés » ou « personnels » dans l'objet de la messagerie de l'agent.

Un message électronique peut être considéré comme un commencement de preuve ou une preuve. Il est donc rappelé que les règles des échanges par écrits s'appliquent à la messagerie. Il est nécessaire de transmettre pour validation à un responsable tout message qui aurait valeur d'engagement.

Il est interdit toute utilisation de la messagerie électronique à des fins illégales. Aussi, aucun message professionnel ou privé ne doit comprendre des éléments de nature offensante, diffamatoire, injurieuse ou à connotation pornographique, sexiste ou raciste.

L'envoi en masse de messages (via « diffusion générale ») n'est pas autorisé, sauf nécessité de service, validée par l'autorité hiérarchique.

2.10.1 Absence de l'utilisateur

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, la DSI peut exceptionnellement, transmettre au supérieur hiérarchique un message électronique réceptionné par son collaborateur s'il n'est pas identifié comme « privé » ou « personnel ». La demande doit au préalable avoir été validée par la Direction des Ressources Humaines.

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), le chef de service peut demander au service informatique, après accord de son directeur, la mise en place d'un message d'absence.

2.10.2 Droit à la déconnexion

L'envoi des messages électroniques est à éviter entre 18h et 8h ainsi que le week-end et les jours fériés.

En-dehors de son temps de travail, l'utilisateur n'est en aucun cas tenu de prendre connaissance des messages qui lui sont adressés ou d'y répondre.

Cependant, ce principe doit être adapté en fonction des cycles de travail des agents ayant des horaires décalés ou étant d'astreinte. De plus, il ne s'applique pas en cas de nécessité de service.

Pendant leurs congés, les agents utilisent la fonction « réponse automatique » pour orienter leurs correspondants vers les collègues en charge de l'intérim de leur poste.

2.10.3 Utilisation de la téléphonie

Les données relatives à l'utilisation des services de téléphonie sont conservées pendant un an conformément à la législation en vigueur. (art. R10-12 à R.10-14 du code des postes et des communications électroniques)

L'utilisation du téléphone (fixe ou mobile) est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles est toléré à condition que cela n'entrave pas l'activité professionnelle.

Le Département se réserve le droit de s'assurer du caractère non abusif de cette utilisation dans les conditions propres à garantir le respect de la vie privée et des libertés des personnels sur le lieu de travail.

Les supérieurs hiérarchiques ne peuvent accéder aux relevés individuels des numéros de téléphone appelés ou des services de téléphonie utilisés que de façon exceptionnelle, en cas d'utilisation manifestement anormale au regard de leur utilisation moyenne constatée au sein du Département.

2.11 Contrôle relatif à l'utilisation des ressources

Le Département se réserve le droit, en cas de suspicion de comportement illicite, d'utilisation frauduleuse, de piratage, ou d'utilisation personnelle manifestement abusive des ressources de faire contrôler par la Direction des Systèmes d'Information, sur ordre écrit de la Direction Générale et après en avoir informé l'agent, les ressources concernées.

L'utilisateur pour lequel de tels faits seraient avérés pourra se voir appliquer des mesures organisationnelles (restriction de l'accès aux ressources informatiques) voire des sanctions disciplinaires, à la demande de sa hiérarchie.
Si l'agent déclare avoir des données à caractère nominatif ou transmises dans le cadre de son travail et pour lesquelles s'imposent le secret professionnel (médecin, travailleurs sociaux, …), un agent de la même corporation sera désigné par la direction concernée afin de prendre connaissance des documents ou messages stockés et vérifier leur contenu au nom de cette même direction.

Le Département se réserve le droit, conformément à la déclaration n°712942 faite auprès de la CNIL, de produire aux utilisateurs, des états statistiques nominatifs d'utilisation des ressources T.I.C. dans l'objectif de veiller à l'intégrité et à la bonne marche du système tout en leur apportant, des indicateurs de consommation des ressources T.I.C. mis à leur disposition.

Ces mêmes états pourront être transmis à titre informatif et de manière anonyme à la Direction Générale ainsi qu'à chaque directeur pour les agents le concernant.

Contrairement à la boîte aux lettres de messagerie, le disque U/ devient un espace de travail récupérable par le service au départ de l'agent. Le service dispose d'un délai de 1 mois pour en faire la demande. En effet les informations contenues sur le U/ sont personnelles à l'agent pour l'exercice de ses missions, mais elles ne sont pas privées.

2.12 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer une continuité de service public, l'utilisateur devra utiliser, pour les activités liées à sa fonction, son adresse électronique professionnelle ainsi que les espaces de stockage partagés mis à sa disposition.

Lors de son départ définitif du service ou de la collectivité, l'utilisateur possédant des droits d'accès sur le réseau du Département certifie que les données utiles ont été transférées sur l'espace de partage du service.

Par ailleurs, l'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de la collectivité, il lui appartient de détruire son espace de données à caractère privé, la responsabilité du Département ne pouvant être engagée quant à la conservation de cet espace. Dans le cas où cet

espace de données à caractère privé n'aurait pas été vidé par l'utilisateur, le Département s'engage à ne divulguer aucun des éléments y figurant à des tiers, sauf cas prévus par la réglementation.

Les boîtes aux lettres électroniques des utilisateurs ayant quitté le Département sont supprimées sous un (1) mois, sans vérification de leur contenu, dès que la Direction des Systèmes d'Information est prévenue, du départ de l'utilisateur, par les services et confirmé par la Direction des Ressources Humaines.
Sauf dérogation motivée par le supérieur hiérarchique, cette suppression intervient dès le départ physique de l'agent (congés annuels, CET, …) suivi d'aucune reprise d'activité effective avant la date de radiation des effectifs.
Il appartient à l'utilisateur de transmettre les informations intéressant le service avant son départ.

L'utilisateur doit garantir à tout moment l'accès à ses données professionnelles.

2.13 Accès depuis l'extérieur du système d'information

Pour répondre aux besoins de mobilité des utilisateurs, agents du Département du Haut-Rhin, dans l'exercice de leurs missions, l'accès sécurisé à distance à tout ou partie du système d'information (Messagerie, Intranet, logiciels métiers..) est possible.

Cette fonctionnalité peut être utilisée en dehors des heures habituelles de travail par l'agent, mais elle ne doit en aucun cas être imposée, notamment par le supérieur hiérarchique.

L'utilisation de ces accès à distance doit résulter d'un choix strictement personnel et doit conserver un caractère exceptionnel et ce afin de préserver l'articulation entre la vie privée et la vie professionnelle.

De fait, le temps d'utilisation en dehors des heures habituellement travaillées ne pourra pas être comptabilisé comme du temps de travail, à l'exception de la situation particulière du télétravail.

2.14 Formation

Le Département est chargé d'organiser les formations nécessaires à chaque utilisateur pour lui permettre :

- D'appliquer les règles et prescriptions de sécurité prévues par la présente charte ;
- Le cas échéant, de se préparer ou de s'adapter aux évolutions technologiques.

3 Les administrateurs des systèmes d'information

Le présent article s'applique spécifiquement aux administrateurs du système d'information du Département.

3.1 Définition et mission d'un administrateur des systèmes d'information

Le terme « administrateur » désigne toute personne chargée expressément du bon fonctionnement et de la sécurité des ressources T.I.C. et des données du Département.

Dans le but d'assurer la disponibilité, l'intégrité, la confidentialité et la journalisation des accès aux données, réseaux, systèmes et applications dont il a la responsabilité, l'administrateur met en œuvre les mesures de sécurité nécessaires. Ces mesures doivent respecter la législation en vigueur et leur mise en place est conditionnée par la définition des objectifs de sécurité fixés par le Département et par les moyens pouvant y être affectés.

3.2 L'administrateur et la sécurité des systèmes d'information

Dans le cadre de l'exploitation, la maintenance et le suivi de l'utilisation des ressources T.I.C. de son périmètre d'activité, l'administrateur des systèmes d'information est amené à effectuer des actions spécifiques lui permettant d'assurer la continuité de service.

L'accès aux données personnelles des utilisateurs par l'administrateur ne peut être justifié que par un principe de nécessité, proportionné au but recherché, c'est-à-dire lorsque le bon fonctionnement des ressources T.I.C. ne peut être assuré par d'autres moyens moins intrusifs

Ces actions lui donnent potentiellement accès à l'ensemble des données des utilisateurs. Cependant, dans le cadre de ces missions, les données auxquelles il accède se limitent aux données issues de la surveillance, de l'audit des réseaux et systèmes et/ou des données nécessaires aux diagnostics de dysfonctionnements et aux recherches de malveillances. En cas d'incident, des investigations peuvent cependant l'amener à prendre indirectement connaissance d'informations de nature confidentielle. Si ces données ne sont pas protégées, il est soumis au devoir de confidentialité et au secret professionnel.

Les administrateurs définissent les privilèges d'accès aux ressources, surveillent et analysent tout incident pour engager les actions nécessaires afin d'y remédier.

L'administrateur met en œuvre une procédure de gestion des accès aux ressources ainsi que des mécanismes d'authentifications.

3.3 Droits et devoirs spécifiques

L'administrateur est soumis à la présente charte informatique. Il doit d'une manière générale respecter les règles d'éthique professionnelle et de déontologie, l'obligation de réserve ainsi que le devoir de discrétion. Il est soumis au secret professionnel

Cependant, pour exercer son rôle au sein du système d'information du Département, il a des droits et des devoirs spécifiques.

Aussi dans le cadre de ces missions, l'administrateur a le droit :

- De prendre toute disposition nécessaire au bon fonctionnement des ressources dont il a la charge ;
- D'établir des procédures de surveillance des données, réseaux, systèmes et applications afin de déceler les problèmes ;

- D'accéder à toute information utile (y compris les fichiers de journalisation) à des fins de diagnostic et d'administration du système, en respectant ses engagements de confidentialité et de non divulgation de ces informations.

L'administrateur a également le devoir :

- De rechercher à améliorer la qualité de service et de la sécurité, dans l'intérêt du Département et des utilisateurs ;
- De respecter la plus stricte confidentialité des mots de passe des utilisateurs sous réserve des nécessités de continuité de service ;
- De garder strictement confidentiel son mot de passe administrateur sous réserve des nécessités de continuité de service ;
- De respecter la confidentialité absolue des informations personnelles dont il a eu connaissance dans le cadre de sa mission, ces informations ne pouvant légalement être communiquées qu'aux autorités judiciaires ou aux personnes appartenant à la chaîne hiérarchique ;
- De veiller à ce que les tiers non-autorisés n'aient pas connaissance d'informations à caractère personnel ;
- De mettre en œuvre un système de journalisation des accès aux ressources ayant pour objet d'identifier et d'enregistrer les connexions ou tentatives de connexion à un système d'information aux fins de garantir une utilisation normale des ressources ;
- De refuser de répondre à une demande qui aurait pour conséquence de lui faire commettre une infraction (droit à la vie privée, droit au secret de la correspondance, loi informatiques et libertés…), en dehors des requêtes des autorités judiciaires ;
- De veiller au respect, par les utilisateurs, de la présente Charte.

En vertu de l'article 40 du code de procédure pénale, la hiérarchie est tenue de signaler sans délai au Procureur de la République les délits dont elle a connaissance. A ce titre, la hiérarchie doit pouvoir transmettre tous les éléments qui y sont relatifs.

3.4 Information des utilisateurs

La mise à disposition de ressources s'accompagne nécessairement d'une information auprès des utilisateurs concernés.

La Direction des Systèmes d'information, en tant qu'administrateur du S.I., est donc tenue :

- D'informer les utilisateurs (par intranet, messagerie ou note de service…), dans la mesure du possible, de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des ressources T.I.C. ainsi que les derniers incidents ayant perturbé ou interrompu l'utilisation habituelle des ressources;
- De les informer de toute opération conduisant à accéder à leur poste informatique, et du motif justifiant cette intervention (sauf lorsque la discrétion des opérations est imposée par les autorités judiciaires). Ces opérations permettent généralement à distance de :
  - Détecter et réparer les pannes ;
  - Prendre le contrôle du poste de travail de l'utilisateur ;
  - Suivre l'activité du poste ;
  - Télédistribuer des logiciels ;
  - Effectuer un inventaire des logiciels installés avec détection des logiciels non autorisés.

4 Règles relatives à la mise en œuvre de la présente Charte

La présente Charte, soumise à l'avis du C.T.P. en date du 27 septembre 2017, abroge la précédente version et entre en vigueur à compter du 1er novembre 2017.

Lorsqu'un compte est ouvert pour un utilisateur, celui-ci doit déclarer avoir pris connaissance de la présente charte, et s'engager à la respecter.

La Charte est portée à la connaissance des utilisateurs par tous moyens et notamment :

- par déclaration électronique de prise de connaissance de la présente charte via l'exécution d'une application informatique ;
- par remise d'un exemplaire papier de la Charte, donnant lieu à un récépissé, dans chaque dossier de recrutement ;
- par voie d'annexe aux conventions et marchés publics dont l'exécution implique l'accès aux ressources T.I.C. du Département, donnant lieu à un récépissé.

L'acceptation de cette charte est obligatoire pour accéder aux ressources T.I.C. du Département du Haut-Rhin.

La présente Charte sera disponible en consultation, à tout moment, sous une ressource partagée (intranet …).

Le suivi de la présente Charte sera assuré par la Direction des Systèmes d'Information (veille juridique et technologique).

Toute procédure de révision de la présente Charte se fera en concertation avec les représentants du personnel.

5 Annexes

5.1 Annexe 1 : modèle de récépissé (à utiliser uniquement par les agents et partenaires n'étant pas en capacité de procéder à la signature électronique du récépissé lors de la connexion à leur session informatique).

Direction des Systèmes d'Information

Conseil départemental Haut-Rhin

Récépissé
de la Charte d'Utilisation des Ressources T.I.C.

Pour les utilisateurs internes du Département
NOM - Prénom :
Direction / Service :

Par les partenaires externes
NOM - Prénom :
Nom de l'organisme / société

Déclare avoir bien pris connaissance des dispositions de la charte d'utilisation des ressources T.I.C. qui m'a été notifiée et m'engage à m'y conformer.

A _____, le _____ / _____ / _____

Signature

Le Département du Haut-Rhin met en place un traitement destiné à suivre les retours de récépissés de prise de connaissance de sa charte d'utilisation des ressources T.I.C.
Conformément à la loi « informatique et libertés » du 6 janvier 1978, chaque utilisateur bénéficie d'un droit d'accès et de rectification aux informations le concernant ; droit qu'il peut exercer en s'adressant à la Direction des Systèmes d'Information : par voie postale au 100 avenue d'Alsace BP 20351 68006 Colmar cedex ou par courriel informatique@haut-rhin.fr

5.2 Annexe 2 : Principaux textes juridiques de référence

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Dispositions Pénales applicables en cas de non respect :
Code Pénal (partie législative) : art. 226-16 à 226-24
Code Pénal (partie réglementaire) : art. R625-10 à R625-13

Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires

Dispositions Pénales applicables en cas d'atteintes aux systèmes de traitement automatisé de données :
Code Pénal (partie législative) : art. 323-1 à 323-7

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

Le Code de la propriété intellectuelle et notamment les articles L335-3 et R.335-5

Le Code des postes et des communications électroniques et notamment les articles R10-12 à R 10-14