Ville d'Esch-sur-Alzette

CHARTE RELATIVE A LA GESTION DES RESSOURCES INFORMATIQUES

Informations générales	
Version :	1.0
État :	
Projet :	28.01.2016
Mise en vigueur :	26.02.2016

PREAMBULE

Considérant que l'Administration Communale de la Ville d'Esch-sur-Alzette se voit confrontée à une évolution fulgurante en ce qui concerne l'usage des ressources informatiques ;

Que les courriels constituent désormais un outil officiel de communication dans le domaine de la bureautique.

Que dans un souci de sécurité et de protection de la santé de ses travailleurs, elle souhaite encadrer l'utilisation de ces outils de travail, afin d'en garantir une utilisation confiante, responsable et dans le respect d'autrui.

Qu'en effet, dans un souci de préservation de la santé de ses employés et fonctionnaires, la Ville se doit de restreindre certains comportements à risques pouvant provoquer, dans le temps, des conséquences néfastes sur le bien-être de ses collaborateurs.

Les Utilisateurs veillent à ce que les règles imposées par le présent règlement soient respectées par toute personne à laquelle ils permettraient d'accéder au système d'information et de communication de la Ville.

DEFINITIONS

On entend par :

« La Ville » = l'Administration Communale de la Ville d'Esch-sur-Alzette

« Les Utilisateurs » = les stagiaires, fonctionnaires, salariés, employés privés en fonction auprès de la Ville ainsi que toute personne tierce ayant accès aux ressources informatiques mises à disposition par la Ville, tel que le personnel enseignant de la Ville.

1 Usage conforme des outils informatiques

Les outils informatiques (hardware et software) sont mis à disposition par la ville pour les besoins du service et à des fins professionnelles uniquement. L'utilisateur doit en faire un usage strictement professionnel et en bon père de famille.

La Ville décline toute responsabilité en cas d'usage dudit matériel à des fins autres que professionnelles et non conformes à sa destination.

Toute infraction pénale commise à l'aide ou au moyen des outils informatiques mis à disposition sera immédiatement dénoncé aux autorités judiciaires.

La Ville ne saurait être tenue pour responsable des dommages causés, respectivement des infractions commises en cas d'usage des outils informatiques à des fins autres que professionnelles.

2 Usage privé au travail

Il est reconnu un droit d'usage privé des moyens mis à disposition par la Ville, seulement s'il est utilisé dans des limites du raisonnable et d'une façon responsable. Cet usage ne doit occasionner aucun trouble ou dysfonctionnement du système d'information et ne doit ni perturber le travail de l'employé lui-même, ni celui de ses collègues.

3 Usage du système d'information

Les règles suivantes doivent être respectées :

- Il est interdit d'utiliser les ressources de la Ville à des fins qui pourraient nuire à l'intégrité de personnes physiques ou morales ou à l'image de la Ville ;
- La législation en vigueur est connue de tous et appliquée ;
- Les Utilisateurs ne peuvent sans autorisation préalable, outrepasser les droits et autorisations qui leur ont été attribués, c'est-à-dire modifier, reproduire, détruire ou lire des informations qui ne leur sont pas destinées ;
- Les Utilisateurs doivent collaborer avec les personnes responsables de la maintenance, afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant survenir ;
- Le matériel mis à disposition des Utilisateurs sera utilisé, manipulé ou stocké avec les soins nécessaires pour éviter toute détérioration ;
- Les Utilisateurs ne peuvent sans autorisation préalable, sortir du matériel ou de l'information de l'enceinte des locaux de la Ville où ils se trouvent.

4 Gestion des mots de passe

Le mot de passe doit :

- Être changé de façon régulière (au moins 1 fois par an) ;
- Avoir une longueur minimale de 8 caractères ;
- Être composé au minimum de lettres majuscules, minuscules et de chiffres ainsi que des signes de ponctuation.

L'Utilisateur est personnellement responsable de la protection de son mot de passe. Il lui est interdit :

- De garder au-delà de la première utilisation, les mots de passe attribués par défaut ;
- D'utiliser des mots de passe facile à deviner (nom de l'Utilisateur, le nom d'un animal domestique, une date de naissance, un numéro de téléphone, mot du dictionnaire, etc.) ;
- D'utiliser le même mot de passe pour plusieurs systèmes ;
- De donner son mot de passe à qui que ce soit ;
- D'envoyer ou de divulguer un mot de passe par email, téléphone, Internet, etc. ;
- De noter le mot de passe sans pour autant le protéger de la façon convenable.

Les comptes génériques connus par plus d'une personne sont également proscrits.

Une dérogation existe toutefois, pour les systèmes n'acceptant pas ces contraintes (code PIN d'un smartphone, par exemple).

5 Usage du matériel électronique

Les Utilisateurs qui ont à leur disposition un ordinateur s'engagent à :

- Protéger l'accès à l'ordinateur par un mot de passe (ou code PIN pour les smartphones) ;
- Bloquer l'accès à l'ordinateur avant de quitter le poste de travail, même pour un très court laps de temps ;
- Ne pas laisser l'ordinateur à des personnes tierces, excepté aux personnes qui ont en charge sa maintenance ;

- Ne pas installer de logiciel sans autorisation ;
- Prendre les dispositions nécessaires, pour sauvegarder les informations stockées éventuellement sur leur poste local (pas de backups).

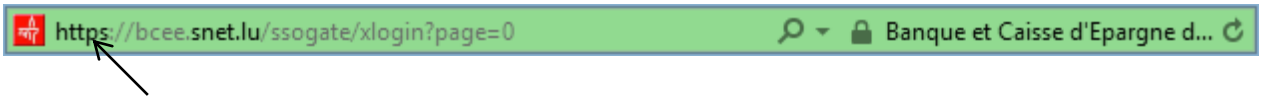
Les Utilisateurs sont conscients que les informations personnelles éventuellement stockées sur le réseau ou dans les emails sont sauvegardées et conservées selon la politique de backup en vigueur.

6 Usage des services internet (web)

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 informatique qui est habilité à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

L'usage d'internet doit se faire en respectant les règles suivantes :

- Lorsque l'Utilisateur saisit des informations sensibles, il doit vérifier qu'il est bien sur le bon site en contrôlant sa barre d'adresse. De plus, pour éviter l'interception de données, il s'assurera que la connexion est sécurisée, notamment par la présence d'un cadenas sur son navigateur et que le l'URL de la page commence par « http**s »**
  Exemple :



- Il est interdit à tout Utilisateur de surfer sur des sites à caractères insultants, racistes, pédophiles, diffamatoires, violents, ou qui nuiraient à autrui ou ne respectant pas la loi ;
- Le téléchargement qui pourrait nuire au système d'information, ou ne respectant pas la législation sur les droits d'auteurs est interdit. En cas de doute, il faut s'abstenir.

7 Usage du courrier électronique et du matériel informatique en général

Les courriers électroniques, tout comme les courriers traditionnels, sont soumis à des règles :

7.1 L'envoi d'e-mails

Lors de l'envoi de courriels, tout Utilisateur doit :

- Indiquer clairement le sujet du message dans la zone « Objet » - si nécessaire avec une des précisions suivantes :
  - ✓ Pour information
  - ✓ Pour avis
  - ✓ Pour instruction / pour attribution et suites à donner

- En cas d'urgence, l'indiquer dans la zone « Objet », tout en sélectionnant la rubrique « Importance haute » - ATTENTION : éviter l'usage abusif de ces outils.
- Etre bref et bien situer le contexte du message afin de garantir que l'on soit bien compris
- Rester courtois en toutes circonstances : les règles de politesse doivent être les mêmes que pour un courrier classique

- Eviter de faire usage abusif de caractères en majuscules et de points d'exclamations pouvant être considéré comme agressif
- S'assurer que sa signature (générée par le système) se trouve bien au bas de son courriel
- Eviter d'envoyer des pièces jointes trop volumineuses – la capacité d'envoi est limitée
- Relire attentivement son texte avant de l'envoyer (et s'assurer que la pièce jointe est effectivement attachée au message)
- Si besoin est, demander un accusé de réception du courriel à travers l'outil « OUTLOOK » conçu à cet effet
- S'assurer que le courriel est uniquement adressé aux personnes concernées – éviter les mises en copie (« Cc ») inutiles.
- Eviter autant que possible de faire usage du champ « Cci » qui désigne des destinataires invisibles par les autres destinataires.

Toujours dans un **souci de respect, de protection de la santé et de bien-être au travail**, la Ville tient à inciter les Utilisateurs à faire un usage parcimonieux et responsable des outils informatiques mis à disposition en dehors des heures de travail. En cas d'urgence le téléphone est à privilégier comme outil de communication. En outre nous invitons fortement les Utilisateurs à mettre en place des messages d'absence de bureau au besoin par le biais des programmes à disposition, tels que OUTLOOK, PROCALL, etc.

7.2 Correspondance privée

L'utilisation de la boîte électronique professionnelle doit principalement et avant tout être utilisée pour la correspondance électronique de nature professionnelle.

L'usage pour besoins personnels doit se faire de manière tout à fait subsidiaire.

En cas d'envoi privé, veiller à ce que la mention « PRIVE » soit précisée dans l'objet.

7.3 Réception d'emails

Tout Utilisateur se doit de :

- Relever sa boîte mail régulièrement
- Ne pas ouvrir de liens contenus dans les mails si la source n'est pas de confiance
- Accuser réception du courrier et traiter les messages dans un délai raisonnable
- Informer son correspondant de toute erreur d'envoi en lui retournant son e-mail
- Traiter tout courriel entrant de manière confidentielle, sauf en cas de nécessité de collaboration
- Supprimer définitivement tout courriel qui ne lui est pas destiné
- En cas de réception répétée d'emails non sollicités ou déplacés, contactez le service informatique pour vous en débarrasser

7.4 Gestion d'emails et archivage

Tout Utilisateur doit, dans le cadre de la gestion de son compte :

- Eliminer régulièrement et définitivement les emails qui ne lui sont pas destinés et/ ou qui ne sont plus d'aucune utilité
- Eviter l'impression de courriel : il convient de favoriser l'archivage informatique

- Adopter un système de classement approprié des courriels importants en fonction de ses besoins, respectivement de ceux du service

7.5 Comportements à prohiber

- La propagation de spams, chaînes de courriers et autres est prohibée ; il est fait appel au bon sens des Utilisateurs.
- Il est fortement déconseillé de mettre sa hiérarchie, ses collègues ou des tiers en « Cci », sous peine de nuire à la bonne entente interne ou de ternir la bonne image de la Ville véhiculée vers l'extérieur
- Il est interdit de transmettre un message confidentiel à un tiers
- Ne pas oublier que l'e-mail sera envoyé sous l'adresse *@villeesch.lu* : l'envoi de contenu susceptible de porter atteinte à la bonne image de la Ville est strictement prohibé.
- L'envoi d'emails par le compte d'un collègue est strictement interdit

7.6 Matériel informatique à disposition des Utilisateurs

Le matériel informatique mis à disposition des Utilisateurs appartient à la Ville.

7.7 Usage de l'outil WORKFLOW – demande de décision

Afin d'assurer un fonctionnement cohérent et efficace de l'outil WORKFLOW, toute demande de décision à adresser au collège des bourgmestre et échevins, respectivement au conseil communal, doit obligatoirement être transmise par WORKFLOW, par le biais de l'application « ***demande de décision*** ».

Toutes demandes adressées par un autre moyen (par porteur, par mail, etc.) ne seront pas prises en compte.

8 Utilisation d'un Laptop ou d'un Smartphone

8.1 Règles communes d'un Laptop d'une tablette ou d'un Smartphone

Toutes les consignes valables pour les ordinateurs de bureau sont à respecter pour les Laptops et les Smartphones. De plus, le caractère nomade de ceux-ci requiert une attention toute particulière de l'Utilisateur qui en a la responsabilité.

Dans le cas d'une attribution permanente ou temporaire d'un appareil, les Utilisateurs concernés ont pour obligation de :

- Respecter les mêmes consignes que celles des ordinateurs de bureau
- Prendre toutes les mesures appropriées pour assurer la sécurité physique des appareils portables mis à disposition, notamment de prévenir tout vol ou dommage physique ;
- Ne pas se connecter à des réseaux informatiques dont le niveau de confiance est inconnu ;
- Effectuer des sauvegardes, lorsqu'il stocke des données sur son appareil portable ;
- Veiller à ce que personne ne puisse voir d'informations confidentielles, lorsque l'appareil est utilisé dans un lieu public ;
- Ne pas utiliser de WiFi privé au sein de la Ville ;

- Désactiver les moyens de communication sans fil (Wifi ou Bluetooth), y compris la recherche automatique de périphérique, lorsqu'ils ne sont pas utilisés ;
- Utiliser le mode de sécurité Bluetooth qui chiffre le trafic dans les deux directions.

8.2 Règles spécifiques aux Laptops

En plus des règles citées ci-dessus, les Utilisateurs qui disposent des Laptops ont pour obligation de :

- Utiliser un câble antivol, s'il est indispensable de laisser le Laptop sans surveillance dans des endroits publics ;
- Prendre le Laptop comme bagage à main lors des voyages ;
- Utiliser un compte Utilisateur spécifique disposant de droits restreints, pour accéder à Internet via son Laptop dans les lieux publics tels que les hôtels, les gares, les aérogares, etc. ;
- Ne pas entraver le fonctionnement de l'antivirus et du pare-feu, et vérifier qu'ils sont activés et régulièrement mis à jour.

Les Laptops sont attribués aux personnes qui, de par leurs attributions, sont amenées à voyager ou à participer à des foires ou des séminaires au Luxembourg comme à l'étranger.

8.3 Règles spécifiques aux Smartphones et tablettes

8.3.1 Règles générales

En plus des règles citées ci-dessus, les Utilisateurs qui font usage des Smartphone ont pour obligation de :

- Connaître les risques principaux liés aux Smartphone, qui sont en l'occurrence, la perte, la divulgation ou la destruction d'information qui sont généralement facilitées par la taille réduite de l'appareil ;
- Protéger l'accès au Smartphone par un code PIN personnel ;
- Mettre à jour avec les nouvelles versions de logiciels, dès qu'elles sont disponibles.

8.3.2 Accès Email sur SMARTPHONE et synchronisation

Il est possible d'installer le compte email professionnel sur son téléphone portable, dit « smartphone »,

Veuillez noter que :

- Par son installation, vous acceptez tacitement le risque lié à une éventuelle panne du système pouvant conduire, au pire des cas, à l'effacement de tout ou partie des données contenues sur ledit appareil ;
- Vous acceptez tacitement qu'en cas de perte, vol du téléphone portable, le service informatique procède à l'effacement à distance des données sensibles en lien direct avec le travail ;

La Ville, en contrepartie, s'engage à traiter les données éventuellement recueillies de manière conforme à la législation en vigueur relative à la protection des données.

8.4 Installation de logiciel

Il est interdit de télécharger ou d'installer soi-même des logiciels non autorisés par le service informatique.

8.5 Utilisation de l'accès à distance de la Ville

Les Utilisateurs d'accès à distance ont à leur charge de contracter les services d'un fournisseur d'accès Internet et de supporter les frais associés.

De plus :

- Ils ont la responsabilité de s'assurer que des Utilisateurs non autorisés ne peuvent pas utiliser leurs droits ou leur infrastructure personnelle pour se connecter au réseau de la Ville ;
- Lorsqu'une connexion à la Ville est établie, l'Utilisateur ne doit en aucun cas, établir d'autres connexions avec d'autres sites distants, ceci pour éviter que l'ordinateur de l'Utilisateur ne serve de pont pour les logiciels malveillants ;
- L'ordinateur utilisé pour se connecter aux systèmes informatiques de la Ville doit disposer d'un antivirus régulièrement mis à jour (p.ex. McAfee, Avira, Norton, Microsoft …) ;
- En utilisant l'accès distant de la Ville, l'Utilisateur doit comprendre que son ordinateur est un prolongement du réseau de la Ville. Il est donc sujet aux mêmes règles et règlements qui s'appliquent aux équipements de la Ville. L'ordinateur doit être conforme à la politique de sécurité de la Ville ;
- Dans le cas de télétravail par exemple, l'Utilisateur doit s'assurer qu'aucune tierce personne n'accède aux biens de la Ville via son accès distant, qu'il n'exerce aucune activité illégale, et n'emploie pas l'accès pour des intérêts commerciaux ou autres. L'Utilisateur est responsable des conséquences de tout abus ;
- Une connexion inactive pendant 30 minutes est automatiquement fermée. L'Utilisateur doit alors rouvrir une nouvelle session. L'utilisation de techniques qui permettent de laisser la connexion ouverte est formellement interdite (ping périodique, etc.) ;
- Toutes les connexions d'accès à distance ont une durée de connexion limitée à 24 heures. Au-delà, l'Utilisateur doit alors rouvrir une nouvelle session ;
- Les programmes utilisés pour gérer la communication distante ne peuvent être que ceux qui ont été approuvés par le service informatique de la Ville.

7. Bureau propre

Les papiers et supports informatiques amovibles contenant des informations sensibles ne doivent pas être laissés sans surveillance sur les bureaux. Spécifiquement, les papiers doivent être retirés rapidement des imprimantes, télécopieurs ou photocopieurs, et ne doivent pas être jetés dans les poubelles.

Les documents sensibles sont déchiquetés ou déposés dans un conteneur sécurisé.

9 Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ou clé 3G. Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière.

De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles rappelées plus haut.

Enfin, la connexion à internet depuis l'étranger est à limiter aux cas d'urgences professionnelle et soumise à l'autorisation de la hiérarchie.

10 Contrôle des activités

Le système d'information et de communication 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 Ville, 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 et de communication. 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 informatique

De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

11 Mise au rebut

Tout équipement qui est mis au rebut ou réutilisé dans un autre contexte doit être vidé de toutes ses données de façon adaptée à la sensibilité des informations qui s'y trouvent.

12 Entrée en vigeur

La présente charte est applicable à partir du 26 février 2016

Elle a été adopté après concertation avec les délégations du personnel de la Ville.