ANNEXE 8

CHARTE D'UTILISATION DU SYSTÈME D'INFORMATIONS DE LA VILLE DE NAMUR

I. INTRODUCTION - LA SÉCURITÉ DE L'INFORMATION 2

II. PORTÉE DE LA PRÉSENTE CHARTE 2

III. CADRE LÉGAL DE RÉFÉRENCE 3

IV. MODALITÉS D'UTILISATION DES MOYENS PHYSIQUES, INFORMATIQUES ET DE TÉLÉCOMMUNICATIONS MIS À DISPOSITION 4

1. UNE UTILISATION PROFESSIONNELLE 4
2. UNE UTILISATION SÉCURISÉE 5
   - A. Les moyens informatiques 5
     - a) Gestion des accès par login et mot de passe 5
     - b) Le principe de précaution 6
   - B. LA TELEPHONIE MOBILE 7
   - C. Le télétravail / les équipements nomades 7
     - Recommandations 7
     - Mise à disposition de matériel 8
   - D. La gestion documentaire et l'archivage 9
3. UNE UTILISATION RÉGULIÈRE 10
   - A. Devoir de réserve et confidentialité 10
   - B. Protection des droits des individus et des données à caractère personnel 11
4. DE L'UTILISATION À TITRE EXTRA-PROFESSIONNEL 12
   - A. internet 12
   - B. LA TELEPHONIE FIXE 12
   - C. TELEPHONIE MOBILE 12
   - D. UTILISATION DE L'E-MAIL 13
     - a) L'e-mail professionnel nominatif 13
     - b) L'e-mail générique ou « boîte partagée » (BP) 13
     - c) L'e-mail privé 14
     - d) L'e-mail syndical 14
   - E. RECHERCHES DANS LES ARCHIVES 14
5. ABSENCE DE L'AGENT 15
   - A. Absence prévue 15
   - B. Absence non planifiée 15
   - C. Absence et continuité du service 15
6. DEPART DE L'AGENT 16

V. MODALITÉS D'INTERVENTION DES MEMBRES DU PERSONNEL CHARGÉS DE LA GESTION DES RESSOURCES INFORMATIQUES ET DE TÉLÉPHONIE 17

VI. LE CONTRÔLE DE L'UTILISATION DU SYSTÈME D'INFORMATIONS 17

1. GÉNÉRALITÉS 17
2. CONTRÔLE DE L'UTILISATION DES COMPTES INDIVIDUELS, DE L'INTERNET, DU COURRIER ÉLECTRONIQUE 19
3. CONTROLE DE LA TELEPHONIE FIXE ET MOBILE 20
   - LA TELEPHONIE FIXE 20
   - LA TELEPHONIE MOBILE 21

VII. LES RESPONSABILITÉS ET SANCTIONS ENCOURUES EN CAS DE NON-RESPECT DE LA CHARTE 21

I. INTRODUCTION - LA SÉCURITÉ DE L'INFORMATION

L' « information » [1] constitue une ressource essentielle pour la Ville de Namur au même titre que ses ressources matérielles ou financières.

L'information peut prendre bien des formes : orale (conversations, discours, échanges téléphoniques, …), écrite (papier ou imprimé), électronique (sms, réseaux sociaux, bases de données, suite bureautique, photos, site web, vidéos, …). Elle peut être stockée sur papier, sur les serveurs de la Ville ou à l'extérieur, transmise par courrier ou via des moyens électroniques, etc.

Le système d'informations fait référence à tout moyen de stocker, de partager l'information : tout matériel ou support physique/numérique utilisé pour traiter l'information et notamment, les ordinateurs (fixes ou portables), programmes informatiques, logiciels, téléphones (fixes et mobiles), photocopieurs, scanners, etc.

Quelle que soit la forme que prend l'information et quel que soit le moyen par lequel elle est stockée et partagée, elle doit toujours être protégée de manière adéquate.

La sécurité de l'information consiste à protéger l'information et son éventuelle confidentialité contre un ensemble de menaces afin de garantir la continuité des activités métier, minimiser les risques et maximiser la qualité du service offert par la Ville aux citoyens et citoyennes.

La sécurité de l'information est rendue possible par la mise en œuvre de mesures et de contrôles de sécurité appropriés. Ces contrôles de sécurité doivent être établis, implémentés, contrôlés, revus et améliorés continuellement, afin que les objectifs de sécurité de l'information ainsi que les objectifs métiers de l'organisation soient rencontrés.

Dans ce cadre, la Ville poursuit la mise en œuvre d'une véritable gouvernance de l'information, à savoir, une politique de gestion centralisée, sécurisée et unifiée, en mettant en place des règles et des procédures visant à optimiser la sécurité de l'information produite par l'administration, en format papier et sur les serveurs : une gestion des droits d'accès, une politique de sauvegarde et de stockage, un plan de classement, des règles de nommage et des durées de conservation des documents.

II. PORTÉE DE LA PRÉSENTE CHARTE

Les règles prévues par la présente charte s'appliquent à l'ensemble du personnel de la Ville de Namur (en ce compris les stagiaires, les étudiants et étudiantes, les personnes sous « contrat article 60 », les bénévoles, etc.) et plus largement, toute personne y travaillant sous quelque statut que ce soit mais également susceptible d'avoir accès au système d'informations.

Tout en garantissant l'équilibre entre les intérêts de chacun, la présente charte a pour buts :

- de sensibiliser au comportement loyal et responsable servant de référence à tout utilisateur et utilisatrice de l'information de l'administration dans ses relations tant vis-à-vis de ses collègues que vis-à-vis de tiers ;
- de protéger les informations gérées par la Ville ;
- de garantir l'intégrité des systèmes d'information de la Ville ;
- de créer et de conserver un environnement de travail professionnel.

[1] « Indication, renseignement, précision que l'on donne ou que l'on obtient sur quelqu'un ou quelque chose » (Larousse, langue française, www.larousse.fr/dictionnaire)

Elle est applicable à l'égard de tout matériel, support physique papier ou connecté appartenant à ou mis à disposition par la Ville et plus largement utilisé à des fins professionnelles dont les PC (fixes et portables), photocopieurs, scanners, téléphones (fixes et portables), supports amovibles (clé USB, disques durs externes), tablettes, télécopieurs, tout moyen permettant le traitement, la production, la collecte, la diffusion, l'enregistrement et le stockage de l'information, de messages, de données, d'images et de sons.

La présente Charte est une annexe au Règlement de travail de la Ville et, à ce titre, en fait intégralement partie.

III. CADRE LÉGAL DE RÉFÉRENCE

- La Charte des droits fondamentaux de l'Union Européenne, article 7 ;
- La Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales ;
- Le Règlement (UE) 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 ;
- La Constitution belge dont les articles 19 et 22 ;
- Le Code Pénal, articles 240 à 242, 314bis, 443 et suivants, 458 ;
- La Loi sur les archives du 24 juin 1955 modifiée par la loi portant des dispositions diverses du 6 mai 2009 ;
- La Loi du 3 juillet 1978 relative aux contrats de travail ;
- La loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie ;
- La loi du 8 août 1983 organisant un Registre national des personnes physiques ;
- Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement des communications et de télécommunications privées ;
- Loi du 28 novembre 2000 en matière de criminalité informatique ;
- Loi du 11 juin 2002 relative à la protection contre la violence et le harcèlement moral et sexuel au travail ;
- La loi du 13 juin 2005 relative aux communications électroniques ;
- Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination ;
- La loi du 19 avril 2014 portant entre autres sur le droit d'auteur et les droits voisins ;
- Digital Act (Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n°910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur ;
- La Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
- Les arrêtés royaux du 18 août 2010 d'exécution de la loi sur les archives du 24 juin 1955 ;
- Le Code de la Démocratie Locale et de la Décentralisation dont l'article L1123-28 ;
- Le Règlement général des archives de la Ville de Namur du 21 mai 2012 ;
- Le Statut administratif applicable aux agents statutaires des cadre technique, spécifique, administratif et ouvrier du 21 janvier 1998 et ses modifications ultérieures ;
- Les Règles générales administratives applicables aux agents contractuels adoptées en date du 20 avril 2000 ;
- Le Règlement de travail applicable à l'ensemble des travailleurs de la Ville du 30 juin 2004 et ses modifications ultérieures ;
- La Recommandation n°8/2012 du 2 mai 2012 de la Commission de la protection de la vie privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail ;

- Politique de sécurité de l'information et vie privée : télétravail sécurisé (securitesociale.be – version du 7 mars 2017).

IV. MODALITÉS D'UTILISATION DES MOYENS PHYSIQUES, INFORMATIQUES ET DE TÉLÉCOMMUNICATIONS MIS À DISPOSITION

1. UNE UTILISATION PROFESSIONNELLE

Dans le cadre de l'utilisation des moyens physiques, informatiques et de télécommunication dont font partie, entre autres :

- Le poste principal de travail, les serveurs informatiques,
- Les équipements nomades (smartphone, tablettes, PC portables dans le cadre par exemple du télétravail, de tout lieu d'exécution des prestations hors siège social ou d'exploitation, de missions particulières, etc.),
- Les espaces de stockage individuel (armoires, clé USB, disque dur externe),
- Les réseaux locaux,
- L'Internet, les logiciels et applications,
- La messagerie électronique,
- La téléphonie fixe et mobile,
- Les locaux (bureaux, espace de stockage, etc.),
- Les archives,
- …

L'utilisateur, l'utilisatrice s'engage à :

- Utiliser le système d'informations comme outil lié à son activité professionnelle dans l'organisation et non à des fins personnelles lucratives ou non, à des fins de promotion, de publicité ou de démarchage ou dans le cadre d'une activité professionnelle ou politique étrangère à la relation liant l'utilisateur, l'utilisatrice, à la Ville (sous réserve du point relatif à l'utilisation du système d'informations à des fins extraprofessionnelles et des conditions particulières applicables en matière de téléphonie) ;
- Utiliser le système d'informations comme un outil de communication et un vecteur d'informations professionnelles et non pour échanger des correspondances privées (sous réserve du point relatif à l'utilisation du système d'informations à des fins extraprofessionnelles) ;
- À ne mener aucune activité illégale par le biais de l'utilisation du système d'informations mis à disposition ;

L'utilisateur, l'utilisatrice s'engage dès lors, notamment, à ne pas :

- Contourner les systèmes d'accès sécurisés de la Ville en vue d'accéder à des sites non autorisés dont l'accès a été bloqué ;
- Copier les logiciels installés par la Ville ou en modifier les configurations ;
- Participer à des chaînes de courrier électronique (spams, robots, canulars) et procédés analogues, à des jeux, à des paris ;
- Participer, au départ de l'infrastructure de la Ville, à un « forum de discussion » pour des raisons non professionnelles ;
- Diffuser ou télécharger des données en violation des lois protégeant le droit d'auteur ;
- Transmettre des messages en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice à la Ville ou à l'auteur du message originel ;

- Envoyer des messages, consulter des sites Internet, de jeux, ou plus largement de l'information dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de message ou la consultation de sites racistes, révisionnistes, érotiques ou pornographiques, de même que les sites prônant toute forme de discrimination, sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, des convictions philosophiques ou politiques d'une personne ou d'un groupe de personnes ;

2. UNE UTILISATION SÉCURISÉE

L'ensemble des données en lien avec la pratique professionnelle des utilisateurs et utilisatrices (informations, fichiers, documents, …) doit être placé sur les répertoires mis à disposition par les services Support et Réseau informatiques (par exemple, le répertoire « I ») ou au sein d'outils dédiés (gestion documentaire, logiciels métiers, services internes, …).

Les données sur support papier sont traitées, gérées, stockées conformément aux directives édictées par le service de Gestion documentaire et des archives.

Cette localisation organisée des données professionnelles traitées permet, pour les informations numériques :

- Une sauvegarde centralisée et systématique (+ mises à jour) des données de l'institution ;
- De limiter le risque de perte de données en cas de fuite ou de perte d'un outil informatique (PC, PC portable, …).

A. LES MOYENS INFORMATIQUES

La sécurité et la sûreté des moyens informatiques imposent le respect, par les utilisateurs et utilisatrices, des consignes édictées en matière informatique.

a) Gestion des accès par login et mot de passe

Tout utilisateur, toute utilisatrice disposant d'un accès au système d'informations de la Ville reçoit un ou plusieurs logins, user ID ou UID (user identification, nom d'utilisateur) pour le(s)quel(s) il ou elle choisit un/des mots de passe.

Le UID est défini par le ou la gestionnaire du système au niveau des services Support et Réseau informatiques afin de pouvoir gérer plus facilement l'ensemble des accès utilisateurs.

Dans le cadre de leur gestion des systèmes et applications, les services Support et Réseau informatiques peuvent transmettre des mots de passe temporaires aux utilisateurs et utilisatrices et ce, de manière confidentielle.

Dans le cadre de la gestion quotidienne de ses accès et mots de passe, tout utilisateur, toute utilisatrice veille au respect des indications suivantes :

- Le mot de passe est strictement personnel ;
- Il est en principe interdit de communiquer à un tiers tout moyen personnel d'accès ou d'authentification sur le système d'informations (mot de passe, carte d'accès, code, …) sous réserve de cas exceptionnels gérés en concertation avec les services Support et Réseau informatiques, la Direction Générale et la personne déléguée à la protection des données ;
- Il est interdit de tenter de décrypter ou de découvrir le mot de passe d'un autre agent, d'une autre agente ;

- Nul ne peut exiger d'un agent ou d'une agente qu'il ou elle communique son ou ses mots de passe pour quelque raison que ce soit. Si la situation se présente, il s'agit de prendre contact avec sa ou son supérieur hiérarchique ou la personne déléguée à la protection des données ;
- Il y a lieu de respecter scrupuleusement la gestion des accès et en particulier ne pas masquer son identité en se connectant sous le nom ou avec le mot de passe d'un autre utilisateur, d'une autre utilisatrice ;
- Il s'agit de créer ses mots de passe pour l'accès au PC et aux applications à accès restreint, les changer régulièrement et/ou lorsque cela est demandé ;
- L'agent ou l'agente n'utilisera pas un programme permettant de se rappeler ses mots de passe à tout moment (ces programmes sont souvent des utilitaires pouvant eux-mêmes être utilisés par l'extérieur pour trouver les mots de passe) ;
- Il est vivement conseillé de ne pas utiliser deux fois un même code ni de les réutiliser mais bien de les renouveler régulièrement (périodicité au sein de la Ville) ;
- L'idéal est de disposer d'un mot de passe difficile à trouver mais facile à retenir ;
- Il est déconseillé d'inscrire son mot de passe sur son sous-main ou sur un petit papier collé au PC ;
- Lorsqu'il ou elle quitte, même temporairement, son poste de travail, l'agent ou l'agente activera son écran de veille désactivable uniquement en introduisant son mot de passe ;
- Se déconnecter du système d'informations après son utilisation pour éviter toute utilisation abusive d'un poste resté connecté ;

b) Le principe de précaution

Dans cette perspective de sécurisation de l'information, il est nécessaire pour toute agente, tout agent :

- De respecter les consignes d'usage et les règles de sécurité (dont les moyens d'authentification utilisés par l'organisme) renseignées par les services Informatiques ;
- De respecter toute contrainte liée aux interventions techniques, y compris à distance ;
- De signaler le plus rapidement possible aux services Support et Réseau informatiques toute violation, tentative de violation suspectée, anomalie malveillante, risque d'intrusion dans son compte informatique et plus globalement, tout dysfonctionnement informatique anormal (dont l'ouverture impossible de fichiers) ;
- De veiller à ne pas propager de virus informatiques, ne pas ouvrir de fichiers exécutables (fichier .exe) ni télécharger de tels programmes sans l'autorisation des services Informatiques ;
- Dans la mesure du possible, de ne pas connecter du matériel mis à disposition par la Ville à un réseau non géré par celle-ci ou à du matériel qui ne lui appartient pas (en ce compris les clés USB non fournies par la Ville). Ces interdictions ne s'appliquent pas aux utilisateurs, utilisatrices, titulaires d'un équipement mobile mis à leur disposition par la Ville dans le cadre de leur activité professionnelle (télétravail, gardes, …) ;
- De ne pas installer, copier, modifier, détruire des logiciels/programmes sans autorisation ;
- De ne procéder à aucune destruction, dégradation, détérioration de biens/documents/données appartenant à la Ville ou à des tiers en contradiction avec les obligations légales ou directives de gestion documentaire interne ;
- De n'entreprendre aucune action conduisant à entraver, fausser, altérer, détourner ou modifier le fonctionnement ou la configuration d'un système ;
- De ne pas installer ni faciliter l'installation par un tiers de logiciels ou de matériels informatiques n'appartenant pas à la Ville sur le système d'informations sans validation expresse préalable des services Informatiques de la Ville (PC portable, assistant numérique, modem, logiciels de partage ou de messages en réseaux …) ;
- De classer/archiver les données importantes ;

- De garantir au mieux la sécurité du matériel mobile (smartphone, PC portable, clé usb professionnelle, ou tout autre support) contenant des informations confidentielles ;
- De veiller à ne pas se maintenir dans un système ou base de données non autorisé ;
- De n'utiliser aucun moyen personnel de chiffrement ou technique de dissimulation d'informations dans les stockages ou les échanges de données impliquant le système d'informations.

B. LA TELEPHONIE MOBILE

L'utilisation de la téléphonie mobile et surtout des smartphones, engendre de nouveaux risques auxquels les utilisateurs, les utilisatrices, doivent prêter attention.

En ce sens, il y a lieu de respecter les directives suivantes en cas d'accès aux ressources de la Ville par ce biais :

- Veiller à la mise à jour régulière de l'OS (par exemple, Android) du smartphone, des logiciels de sécurité ainsi que de toutes les applications qui y sont chargées ;
- Veiller à ne charger des applications que via des plateformes sécurisées. Toute nouvelle application honnête sollicitera une confirmation des accès aux données personnelles dont elle a besoin. Il s'agit de demeurer parcimonieux et conscient des accès accordés ;
- En cas d'utilisation professionnelle du téléphone mobile privé, s'assurer que l'antivirus est à jour ;
- Veiller à ce qu'une mise en veille automatique soit activée sur le smartphone et qu'il soit nécessaire d'entrer un code secret pour en sortir.

C. LE TÉLÉTRAVAIL / LES ÉQUIPEMENTS NOMADES

- Recommandations

Tel que mis en œuvre par la Ville de Namur, le télétravail se définit comme une forme de travail à domicile, qui peut être régulier ou occasionnel. Il s'agit d'un travail délocalisé grâce au recours aux technologies de l'information et de la communication (TIC), notamment.

Conformément à l'annexe au Règlement de travail relative au télétravail, celui-ci est fixé dans le cadre du contrat de travail (clause, avenant, convention spécifique pour les membres du personnel statutaires).

A l'occasion de la pratique du télétravail, les droits et devoirs applicables à l'ensemble des membres du personnel demeurent valables et d'application dont, notamment, les devoirs de discrétion, de confidentialité, de secret professionnel et de respect du Règlement général sur la protection des données.

Le télétravail s'effectue au domicile ou dans tout autre lieu pour autant que les conditions techniques, de sécurité et de contrôle soient respectées.

Lorsque le recours aux ressources informatiques de la Ville est nécessaire dans le cadre du télétravail, les modalités de connexion à distance doivent être demandées et seront communiquées par le service Réseau informatique.

Lors du télétravail, l'attention des membres du personnel est attirée sur les points suivants :

- Veiller à ne pas utiliser de wifi non sécurisé (souvent le cas des wifi publics, réseaux ouverts non protégés) ;

- Ne pas faire usage/cliquer sur des liens inconnus dans des emails ou pages web et privilégier l'accès à un site internet en inscrivant l'adresse du site directement dans le navigateur ;
- Veiller à ne pas installer/télécharger de logiciels/d'applications malveillants ;
- Veiller à se connecter en direct - en présentiel - au réseau Ville régulièrement et à tout le moins une fois par mois avec le matériel portable mis à disposition afin que puissent s'initier les mises à jour de sécurité ;
- Veiller à la confidentialité des informations visibles depuis l'écran par le biais du verrouillage de celui-ci ;
- Il est déconseillé d'imprimer des informations dans l'environnement externe de télétravail ;
- Il est interdit de stocker des informations professionnelles confidentielles, sensibles en local sur un appareil privé à moins d'être en mesure de procéder à leur chiffrement ;
- Il est interdit de s'envoyer, sur une adresse mail privée, des informations professionnelles confidentielles ou contenant des données à caractère personnel ;
- Veiller à la sécurité et au respect de la confidentialité de toutes les informations sous format papier.

Le télétravail s'accompagne souvent de la mise en place et de l'utilisation d'outils de visioconférence, de chat, …. Il y a lieu de veiller à la confidentialité des potentiels enregistrements réalisés tant sur le PC que sur le cloud.

L'usage de ces outils par les membres du personnel de la Ville doit se faire de manière conforme :

- Aux consignes et aux recommandations spécifiques qui accompagnent leur mise en service ;
- A la philosophie et au prescrit de la présente charte.

- Mise à disposition de matériel

Un inventaire du matériel mis à disposition des membres du personnel (PC portables, PC, tablettes, clés USB cryptées, disques durs externes, …) est tenu à jour par le service Support informatique.

Le service de Gestion immobilière gère la mise à disposition des cartes SIM et le service Ressources logistiques gère la mise à disposition des GSM et smartphones.

En cas de vol ou de perte du matériel, l'utilisateur, l'utilisatrice doit contacter :

- Le service ayant mis à disposition le matériel (le service Support informatique, de Gestion immobilière, Ressources logistiques) ;
- Le service Réseau informatique : aspects sécurité ;
- La personne déléguée à la protection des données : risque de fuite de données à caractère personnel (dpo@ville.namur.be) ;
- Dans l'hypothèse du vol, l'utilisateur doit pouvoir faire état d'une plainte déposée à la police.

Le cas échéant, il ou elle veille :

- Au blocage immédiat de la carte SIM et/ou du dispositif mobile en contactant le service de Gestion immobilière ;
- Au blocage des applications bancaires en appelant Card-Stop (070 344.344).

Le membre du personnel a l'obligation d'informer son employeur, via le service Support informatique ou celui de des Ressources logistiques, des défectuosités / détériorations qu'il ou elle aurait constatées au matériel confié.

Si sa responsabilité est établie, il peut être demandé à l'utilisateur, à l'utilisatrice, d'indemniser la Ville en remboursant la valeur résiduelle du dispositif mobile.

En tout état de cause, en cas de départ de l'administration, d'arrêt des missions pour lesquelles le matériel a été mis à disposition ou de changement vers un nouveau poste pour lequel le matériel n'est plus requis, l'utilisatrice, l'utilisateur, peut être amené à devoir rapporter le matériel ayant été mis à sa disposition et appartenant à la Ville.

D. LA GESTION DOCUMENTAIRE ET L'ARCHIVAGE

L'utilisation du système documentaire (documents en circuit, archives papiers et électroniques) au sein de l'administration se fait dans le cadre des procédures établies par le service Gestion documentaire et dans le respect du règlement communal en vigueur à ce sujet. Les informations sont disponibles sur l'intranet, l'adresse de contact étant archives@ville.namur.be.

Le Service Gestion documentaire donne des directives et des conseils aux services afin de leur permettre de gérer aux mieux leurs documents et leur donner un environnement de travail agréable et sécurisé pour le partage de l'information.

A cette fin, le Service Gestion documentaire suit notamment les règlementations en vigueur et les directives adoptées par les Archives Générales du Royaume.

Pour les documents et données non encore versés au Service Gestion documentaire, ce dernier dispense des conseils de bonne gestion aux membres du personnel.

Ceux-ci sont invités à suivre les recommandations suivantes : plan de classement physique ou sur le serveur, règles de nommage, rangement physique de dossiers, recours aux bordereaux de versement, de destruction et de transfert.

Des boîtes de destruction confidentielles des documents sont mises à disposition des services au sein de l'administration. L'utilisation de ces boîtes pour la destruction des données personnelles est obligatoire.

L'agente, l'agent veille à sécuriser l'accès aux données papiers conservées au sein de son service : locaux fermés, accessibles à certaines personnes clairement identifiées, armoires fermées, journal de suivi de consultation, entre autres.

Les documents et données en format électronique non encore archivés sont conservés sur un serveur sécurisé et selon les meilleures conditions mises à disposition.

Dans le cadre de sollicitations de documents archivés, les membres du personnel veilleront à effectuer des demandes précises et utiliseront les formulaires à leur disposition.

Tout membre du personnel s'engage également à restituer les documents empruntés dans leur intégralité et dans un délai raisonnable.

Le service Gestion documentaire peut refuser toute demande qui ne serait pas conforme aux règlements existants.

3. UNE UTILISATION RÉGULIÈRE

A. DEVOIR DE RÉSERVE ET CONFIDENTIALITÉ

Toute utilisatrice, tout utilisateur s'engage à ne diffuser aucune information personnelle et/ou confidentielle relative à la Ville, à ses partenaires, à ses agents et agentes sauf dans le cadre strict de la conduite des dossiers.

L'utilisateur, l'utilisatrice s'engage à ne divulguer aucune information concernant les activités de la Ville ni aucune donnée relative aux citoyens, citoyennes et/ou membres du personnel dont il pourrait avoir connaissance dans l'accomplissement de ses fonctions et qui serait de nature à porter préjudice à la Ville, aux citoyens, citoyennes ou aux membres du personnel.

Cette obligation de confidentialité s'applique tant à l'égard des tiers que des membres du personnel.

En ce sens, l'article 12 du Statut administratif dispose qu'il est interdit aux membres du personnel « *de révéler des faits qui ont trait à la sécurité nationale, à la protection de l'ordre public, aux intérêts financiers de la Ville, à la prévention et à la répression des faits délictueux, au secret médical, aux droits et libertés du citoyen, et notamment au droit au respect de la vie privée. Cette interdiction vaut également pour les faits qui ont trait à la préparation de toutes les décisions* ».

Cette interdiction gardera tous ses effets pendant toute la durée de la relation de travail et se prolongera après la rupture de celle-ci pour quelque motif que ce soit.

Le membre du personnel se doit également d'exercer ses missions en toute loyauté et intégrité conformément aux articles 13 et 17 du Statut administratif.

Les agentes et agents sous contrat de travail sont soumis à la législation relative aux contrats de travail dont les articles 16 et 17 de la loi du 3 juillet 1978.

L'utilisateur, l'utilisatrice qui recevrait des informations qui ne lui sont pas destinées est tenu d'en respecter la confidentialité. Dans un tel cas de figure, il y a lieu de supprimer le contenu, le message et d'en avertir son expéditeur, son expéditrice.

B. PROTECTION DES DROITS DES INDIVIDUS ET DES DONNÉES À CARACTÈRE PERSONNEL

L'attention des utilisateurs et utilisatrices est attirée sur la législation applicable au traitement de données à caractère personnel : le 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 (ci-après RGPD) ainsi que la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Afin de garantir le droit au respect de la vie privée de chacun, chacune[2], tout traitement[3] de données à caractère personnel[4] opéré au sein de la Ville de Namur doit répondre aux principes suivants (art. 5 du RGPD) :

- La licéité, la transparence et la loyauté,
- La poursuite de finalités déterminées, explicites et légitimes,
- La minimisation et l'exactitude des données,
- La limitation de la conservation,
- La mise en œuvre de mesure de sécurité appropriées (intégrité et confidentialité).

Dans le cadre de la poursuite de la mise en œuvre des mesures et des processus de mise en conformité au RGPD initiés au sein de la Ville de Namur, les agents et agentes veillent à se conformer aux instructions fournies par l'employeur qui, à la lumière du Règlement, dispose de la qualité de responsable de traitement ainsi que par la personne déléguée à la protection des données.

L'agente ou l'agent qui communiquerait, transmettrait des données à caractère personnel à un ou plusieurs destinataires internes et/ou externes au(x)quel(s) ces données n'étaient pas destinées doit, sans délai :

- Prévenir les destinataires,
- Prévenir la personne déléguée à la protection des données de cette fuite de données.

De manière générale, il revient à tout utilisateur, toute utilisatrice, à tout membre du personnel d'avertir la personne déléguée à la protection des données, par le biais du référent, de la référente DPO de son service notamment, de tout incident (fuite, perte, vol) relatif à des données à caractère personnel d'agents, d'agentes ou de tiers (citoyens, …).

[2]Article 7 de la Charte des droits fondamentaux de l'UE ; article 22 de la Constitution.

[3] Consiste en toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

[4] Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une personne physique identifiable, une personne physique qui peut être identifiée, directement ou indirectement, notamment via un nom, un numéro d'identification, des données de localisation, un identifiant ou un élément spécifique se rapportant à l'identité physique, physiologique, génétique, psychique, économique, culturel ou social.

4. DE L'UTILISATION À TITRE EXTRA-PROFESSIONNEL

Un usage non-professionnel du système d'informations dans le cadre des nécessités de la vie courante et familiale est toléré pour peu qu'il soit raisonnable et s'exerce dans les conditions suivantes :

- Que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels ;
- Que l'utilisation d'internet n'entrave pas l'accès professionnel ;
- Que l'utilisation du système d'informations à titre extraprofessionnel ne se fasse pas au détriment des tâches professionnelles ;
- Les utilisatrices, les utilisateurs sont autorisés à conserver une quantité raisonnable de données privées sur le disque réseau (H:) de leur PC.

A. INTERNET

L'usage d'internet, à des fins privées, sans autorisation spécifique de la part de la, du supérieur hiérarchique est toléré.

L'accès à internet à des fins privées doit cependant répondre aux conditions suivantes :

- Il doit être occasionnel et réservé au temps de pause ;
- L'utilisation d'internet doit se faire dans le respect des dispositions prévues au niveau des « Modalités d'utilisation des moyens physiques, informatiques et de télécommunications » et plus globalement, de la présente charte et de toute disposition légale.

B. LA TELEPHONIE FIXE

L'usage de la téléphonie à des fins privées, sans autorisation spécifique de la part de la, du supérieur hiérarchique est toléré pour peu qu'il réponde à une nécessité impérieuse et n'entrave aucunement la bonne conduite des activités de la Ville.

Par nécessité impérieuse sont visés les actes de gestion personnelle qui concernent la santé ou le patrimoine de l'agent, de l'agente ou des membres de sa famille et qu'il est impossible d'accomplir en dehors des heures de travail.

Toute communication téléphonique vers un numéro payant/surtaxé (notamment les numéros commençant par 0900 et 070) est strictement interdite sauf si l'utilisation en est professionnelle et admise par la Ville.

Toute communication téléphonique à l'international est strictement interdite sauf si celle-ci répond à des finalités professionnelles admises par la Ville.

C. TELEPHONIE MOBILE

Les dispositifs mobiles et cartes SIM mis à disposition restent propriété de la Ville.

La mise à disposition de matériel de téléphonie mobile et/ou carte SIM est envisageable dans les conditions définies par le Collège communal et se matérialise par la signature d'une convention de mise à disposition et d'utilisation d'un téléphone professionnel par les agentes et agents communaux ou d'une convention d'utilisation de portable professionnel (appareil, abonnement, data) en cas d'abonnement de type forfait.

Compte tenu de l'évolution technologique et d'une analyse récurrente des nouvelles possibilités tarifaires, les conditions d'utilisation de matériel de téléphonie mobile font régulièrement l'objet de modifications.

Ces conditions de mise à disposition et d'utilisation, en ce qu'elles permettent une éventuelle utilisation du système d'informations à des fins extra-professionnelles, demeurent dès lors régies par les décisions du Collège communal et respectent les dispositions fiscales applicables en la matière.

En tout état de cause, le matériel de téléphonie et/ou la carte SIM mis à la disposition de l'agent ou l'agente ne peut être utilisé qu'à l'usage pour lequel il est délivré.

Les appels téléphoniques vers ou depuis des numéros payants/surtaxés (notamment les numéros commençant par 0900 et 070) ainsi que les appels à l'international sont soit admis par la Ville à des fins professionnelles, soit passés à des fins privées et alors considérés (cas de l'abonnement de type forfait), renseignés et facturés comme tels.

D. UTILISATION DE L'E-MAIL

a) L'e-mail professionnel nominatif

Le membre du personnel qui utilise l'e-mail avec son « adresse nominative Ville » veillera à ce que le contenu soit strictement professionnel sous réserve des dispositions prévues au point « l'e-mail privé ».

Les coordonnées de la signature automatique seront mises à jour et pertinentes. Les nom, prénom, fonction et numéros de téléphone, gsm sont complets, ces données étant utilisées par l'extérieur de la Ville.

La signature automatique est insérée dans tout échange d'e-mails professionnels.

Tout membre du personnel se référera, pour la création de sa signature d'e-mail, à la charte graphique de la Ville de Namur et aux indications utiles en matière de *disclaimer*.

Les agents et agentes qui, en raison de leur fonction, envoient des e-mails en lieu et place d'un ou d'une autre collègue, signent l'e-mail en leur nom propre avec la mention « Pour X ».

b) L'e-mail générique ou « boîte partagée » (BP)

Chaque service reçoit une adresse générique du type service@ville.namur.be. Cette adresse peut être gérée par une ou plusieurs personnes.

L'organisation de la gestion de ces boîtes est laissée à chaque service. Chaque responsable de service veillera à exposer la procédure choisie pour son service.

L'attribution de l'adresse générique du service n'empêche en rien la création et l'attribution d'e-mails génériques ou boîtes partagées propres à des cellules ou projets spécifiques menés au sein du service.

Il est conseillé de privilégier cette adresse dans les en-têtes de courrier et ainsi assurer un suivi de toute correspondance.

Chaque service disposant d'un e-mail générique veillera à mettre en place une réponse automatique de type accusé de réception par l'intermédiaire des services Informatiques.

c) L'e-mail privé

Les membres du personnel veilleront à utiliser leurs comptes de messageries privés pour leurs communications et échanges privés.

Néanmoins, l'usage occasionnel et de brève durée, à des fins privées, du système de messagerie électronique mis à disposition par la Ville et via la boite personnelle de l'agente, de l'agent (et non via une boite générique propre à un service, une cellule ou un projet), est toléré.

Celui-ci ne peut en rien entraver le bon fonctionnement, la productivité et les relations sociales au sein de la Ville ainsi que les relations extérieures à la Ville.

Il ne peut constituer une infraction aux présentes instructions ni aux dispositions légales et réglementaires applicables.

Si l'agente, l'agent fait usage de cette faculté, elle ou il est tenu d'indiquer, dans l'objet du message, que celui-ci a un caractère privé. Il ou elle doit en outre supprimer, dans le corps du message, toute mention relative à la Ville (telle que la signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé dans le cadre de l'exercice des fonctions.

L'agent, l'agente, veillera à ne pas surcharger sa messagerie professionnelle par des éléments qui relèvent de la sphère privée (ex: photographies numériques personnelles, contenus multimédia, ...).

Tout mail avec l'objet «privé» sera:

- soit supprimé automatiquement des éléments envoyés et de la boîte de réception ;
- soit placé dans un répertoire de l'arborescence appelé «Privé».

d) L'e-mail syndical

L'utilisation de l'email par les organisations syndicales et leurs déléguées, délégués est autorisée en vue de la diffusion d'informations entre eux, à leurs affiliés et affiliées, aux Directeurs généraux, au Collège ou au Conseil.

Si les syndicats font usage de cette faculté, ils sont tenus d'indiquer, dans l'objet du message, que celui-ci a un caractère syndical. Ils doivent en outre supprimer, dans le corps du message, toute mention relative à la Ville (telle que la signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé dans le cadre de l'exercice des fonctions.

Tout e-mail avec l'objet « Syndical » sera pour les syndicats comme pour les affiliés et affiliées, placé dans un répertoire de l'arborescence appelé «Syndicat».

E. RECHERCHES DANS LES ARCHIVES

Les recherches dans les archives (recherches généalogiques, administratives, urbanistiques), hors cadre professionnel, ne peuvent être effectuées que sur demande motivée auprès du service concerné.

La demande peut se faire via l'envoi d'un mail à archives@ville.namur.be ou genealogie@ville.namur.be

En fonction de la motivation de la demande et dans le respect de la législation en vigueur, le service Gestion documentaire répond favorablement ou non à la demande des personnes concernées, comme pour tout citoyen, toute citoyenne.

Il n'est en aucun cas autorisé de faire valoir sa position d'agent communal ou d'agente communale pour délivrer à un tiers, des informations provenant des archives sans autorisation utile.

5. ABSENCE DE L'AGENT

A. ABSENCE PRÉVUE

En cas d'absence prévue, tout membre du personnel veillera alors à activer le gestionnaire d'absence, en respectant les recommandations suivantes :

- ✓ Faire usage des fonctionnalités de la boîte de messagerie permettant de définir une réponse automatique pour le message envoyé en interne et celui adressé à l'extérieur ;
- ✓ Indiquer le nom complet du ou de la collègue de contact ;
- ✓ Indiquer le numéro de téléphone complet, ainsi que l'adresse électronique de contact ;
- ✓ Le message doit être mis à jour à chaque absence (attention aux dates) ;
- ✓ Le gestionnaire d'absence doit être désactivé dès le retour si cela ne se fait pas de façon automatique.

B. ABSENCE NON PLANIFIÉE

En cas d'absence non planifiée d'un membre du personnel, une procédure de réponse automatique d'absence sera installée, à la demande écrite du Chef, de la Cheffe de service, par les services Informatiques.

Les demandes sont à adresser à l'adresse renseignée, accompagnées d'un texte pré-rédigé par le, la responsable de service sur le modèle repris ci-dessous :

Bonjour,
M./Mme X…… est actuellement absent(e).
Merci d'envoyer vos courriels à l'adresse suivante : ……
Pour toute urgence, vous pouvez également contacter le ……
Merci d'avance.
Signature de la Cheffe, du Chef de service

Cette procédure n'implique pas que les services Informatiques pénètrent dans la messagerie de l'agent ou de l'agente concerné(e).

C. ABSENCE ET CONTINUITÉ DU SERVICE

En tant qu'institution publique et employeur, la Ville de Namur doit pouvoir gérer les communications de son organisation et garantir, en tout temps, la continuité de ses missions de service public.

Pour ce faire, en cas d'absence planifiée ou non d'un agent ou d'une agente, pour laquelle celui-ci ou celle-ci n'aurait pas pris ou pas pu prendre les dispositions utiles (nettoyage de la boîte mail, message d'absence, transfert des courriels utiles à ses collègues) et dès lors susceptible de mettre en péril la poursuite des services d'intérêt public, la Directrice générale peut déléguer, sur base d'une demande écrite motivée de la ligne hiérarchique, l'accès à la messagerie de l'agent ou de l'agente dont question à sa, son responsable hiérarchique ou à un autre membre de son service.

Le supérieur, la supérieure hiérarchique veillera à mettre en copie ou à informer par écrit la personne déléguée à la protection des données de la demande exprimée en ce sens à la Directrice générale.

Il y a lieu de préciser que cette situation n'entre pas dans le cadre d'un examen suite à une anomalie ou d'un contrôle mais se justifie exclusivement par l'urgence de la situation et la poursuite nécessaire du service public.

Il peut notamment s'agir des cas d'absences de longue durée (interruption de carrière et toutes causes de suspensions de l'activité professionnelle à temps plein).

L'agente, l'agent dont l'accès à la messagerie a été concédé en est informé au plus vite par sa ou son supérieur hiérarchique.

6. DEPART DE L'AGENT

En cas de départ d'un agent, d'une agente (rupture de la relation de travail, départ à la retraite), la Ville de Namur doit en tout temps assurer la continuité de ses missions de service public.

Pour ce faire, l'agent, l'agente doit activer le gestionnaire d'absence via un message automatique qui avertira tout correspondant ultérieur (interne et externe) du fait que la personne concernée n'exerce plus ses fonctions au sein de la Ville et renseignera les coordonnées de la personne (ou adresse mail générique) à contacter en ses lieu et place.

Dans le cas où l'agent, l'agente n'a pas activé le gestionnaire d'absence dans les conditions décrites ci-dessus, une procédure de réponse automatique d'absence sera installée, à la demande écrite du Chef, de la Cheffe de service, par les services informatiques.

Les demandes sont à adresser à l'adresse renseignée, accompagnées d'un texte pré-rédigé par le, la responsable de service sur le modèle repris ci-dessous :

> *Bonjour,*
> *M./Mme X…… a cessé ses fonctions au sein de la Ville de Namur.*
> *Merci d'envoyer vos courriels à l'adresse suivante : …….*
> *Pour toute urgence, vous pouvez également contacter le …….*
> *Merci d'avance.*
> *Signature de la Cheffe, du Chef de service*

Cette procédure n'implique pas que les services informatiques pénètrent dans la messagerie de l'agent ou de l'agente concerné(e).

En tout état de cause la messagerie électronique de l'agent, l'agente sera bloquée au plus tard le jour de son départ effectif.

Le message automatique indiquant que l'agent, l'agente a cessé ses fonctions au sein de la Ville de Namur sera envoyé pendant une période de temps raisonnable, *a priori* 1 mois.

Toutefois, en fonction du contexte et, en particulier, du degré de responsabilité exercé par la personne concernée (telle qu'une fonction de chef, cheffe de département, chef, cheffe de service) un délai plus long peut-être admis et ne pouvant idéalement pas dépasser 3 mois.

Au-delà de cette période, la messagerie électronique de la personne concernée sera supprimée.

V. MODALITÉS D'INTERVENTION DES MEMBRES DU PERSONNEL CHARGÉS DE LA GESTION DES RESSOURCES INFORMATIQUES ET DE TÉLÉPHONIE

Le Collège désigne les fonctions habilitées, en vertu de la présente instruction, à exercer sur le système d'informations une mission de contrôle, d'examen, de maintenance ou d'assistance.

Ces agentes et agents ne pourront accéder qu'aux seules données dont elles/ils ont besoin pour l'exercice de ces missions et ne pourront les communiquer que dans le respect des procédures écrites se rapportant à leurs missions.

Dans le cadre de l'exercice de ces missions et tâches, elles/ils sont tenus à un devoir de confidentialité et s'exposent à des sanctions en cas de violation de celui-ci.

Les administrateurs, administratrices systèmes et les personnes disposant de privilèges avancés sur les systèmes d'information sont tenus de signer le code de déontologie spécifique à leur mission.

La personne déléguée à la protection des données est tenue de respecter le Code de déontologie des Délégués, Déléguées à la protection des données dès celui-ci adopté et publié par l'Autorité de protection des données.

VI. LE CONTRÔLE DE L'UTILISATION DU SYSTÈME D'INFORMATIONS

1. GÉNÉRALITÉS

Le contrôle de systèmes d'informations et de leur utilisation est effectué de manière ponctuelle, il peut être global (sans individualisation des utilisateurs, utilisatrices dont les membres du personnel) ou ciblé (examen de l'utilisation réalisée par un utilisateur, une utilisatrice ou plusieurs, dont les membres du personnel).

Les données personnelles en lien avec l'utilisation des systèmes d'informations (durée de connexions informatiques, date et heure d'ouverture et de fermeture de session, URL des sites visités, numéros composés, logs aux différents outils, …) sont des informations collectées et conservées au sein de la Ville. La durée de conservation de ces données varie selon les dispositifs concernés.

Cette collecte et ce stockage de données sont, entre autres, motivés par des objectifs de continuité du service, de contrôle du bon fonctionnement des systèmes informatiques, de back-up, de sécurité, de traçabilité et de facturation.

Ces données peuvent être utilisées, moyennant le respect des législations et procédures établies, lors de contrôles généraux des systèmes d'informations et lors d'examens individualisés de l'utilisation des systèmes d'informations réalisée par un utilisateur, une utilisatrice, voire plusieurs.

La Ville de Namur est fortement attachée au principe du respect de la vie privée des utilisateurs, des utilisatrices, dont les membres du personnel et veille à respecter scrupuleusement les principes du Règlement Général sur la Protection des Données ainsi que le prescrit de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Lorsque les agentes et agents désignés à cette fin, entreprennent le contrôle de systèmes d'informations et/ou de l'utilisation faite de ceux-ci par un utilisateur, une utilisatrice, elles/ils s'engagent à les réaliser dans le strict respect du droit à la vie privée et de la protection des données à caractère personnel.

Tout contrôle est mené dans le respect des principes de finalité, de proportionnalité et de transparence tels que prévus dans la réglementation relative à la protection de la vie privée.

Principe de finalité

Le contrôle des systèmes d'informations ne peut se réaliser que pour autant que l'une ou plusieurs des finalités suivantes est ou sont poursuivie(s):

a. la sécurité et/ou le bon fonctionnement technique des systèmes d'informations en réseau de la Ville, ainsi que la protection physique des installations ;
b. la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
c. la protection de la réputation des intérêts économiques et financiers de la Ville ;
d. le respect des principes et règles d'utilisation des systèmes d'information de la Ville tels que fixés dans la présente Charte.

Principe de proportionnalité

La Ville de Namur respecte le principe de proportionnalité dans la poursuite de ces finalités.

Le contrôle des systèmes d'informations ne peut entraîner une ingérence dans la vie privée de l'utilisateur, de l'utilisatrice ou, tout au plus, une ingérence réduite au minimum et dûment motivée.

Ainsi, ne seront traitées, collectées, examinées en vue du contrôle des systèmes d'informations que les données qui sont nécessaires, indispensables au contrôle et qui ont de surcroît, un caractère adéquat, pertinent et non excessif par rapport aux finalités poursuivies.

Les contrôles globaux des systèmes d'informations se feront sur base de données ne permettant pas d'identifier les utilisateurs individuellement.

Principe de transparence

Les modalités de contrôle définies dans la présente Charte sont portées à la connaissance de l'ensemble des utilisateurs et utilisatrices des systèmes d'informations.

Pour les membres du personnel, la Charte fait en effet partie intégrante du Règlement de travail mais elle est aussi portée à leur connaissance de manière individuelle:

- La Charte est présentée lors de toutes les séances d'accueil des nouveaux membres du personnel à l'issue desquelles un exemplaire est remis à chacun et chacune, ce dont atteste la certification de participation délivrée à l'issue des séances d'accueil ;
- Tout nouveau membre du personnel se connectant pour la première fois sur sa session personnelle doit cocher une case précisant qu'il déclare avoir pris connaissance de la Charte ;
- La Charte fera l'objet d'une communication appropriée à l'ensemble du personnel dès son entrée en vigueur ;
- La Charte est disponible sur le site internet de la Ville ainsi que sur l'Intranet ;

Le contrôle des comptes utilisateurs, des emails professionnels et de l'utilisation d'internet est réalisé sur base de la recommandation n°8/2012 du 2 mai 2012 de la Commission de la protection de la vie privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail.

2. CONTRÔLE DE L'UTILISATION DES COMPTES INDIVIDUELS, DE L'INTERNET, DU COURRIER ÉLECTRONIQUE

Lorsque, à l'occasion d'un contrôle non individualisé ou au départ d'autres sources d'information, il est constaté ou suspecté une anomalie[5], un usage interdit, abusif ou excessif d'un ou de plusieurs comptes utilisateurs, de l'accès à internet ou du système de courrier électronique, l'agente ou l'agent désigné responsable du contrôle en informe, par écrit, son Chef ou sa Cheffe de service et, en concertation, ils évaluent le risque et le suivi à y apporter.

Si l'anomalie, l'usage interdit, abusif ou excessif d'un ou de plusieurs comptes individuels, de l'accès à internet ou du système de courrier électronique constaté ou suspecté est en lien avec la poursuite, par la Ville, d'une ou de plusieurs des finalités a), b) et c) reprises au point VI.1, il pourra être procédé directement à l'identification et à l'individualisation des données des utilisateurs, utilisatrices, membres du personnel, par l'adresse IP, le login ou tout autre moyen nécessaire.

Pour rappel, ces finalités sont les suivantes :

a) la sécurité et/ou le bon fonctionnement technique des systèmes d'informations en réseau de la Ville, ainsi que la protection physique des installations ;
b) la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
c) la protection de la réputation des intérêts économiques et financiers de la Ville.

Si l'anomalie, l'usage interdit, abusif ou excessif d'un de plusieurs comptes utilisateurs, de l'accès à l'internet ou du système de courrier électronique constaté ou suspecté est en lien avec la poursuite, par la Ville, de la finalité d) reprise au point VI.1, il ne pourra être procédé à l'identification et à l'individualisation des données des utilisateurs, utilisatrices, membres du personnel, qu'après une phase préalable d'information et après récidive. Cette information, sous forme de rappel des principes et règles en vigueur au sein de l'entreprise a pour objectif de porter à la connaissance des utilisateurs, des utilisatrices de manière claire et compréhensible, l'existence d'une irrégularité et de les avertir d'une individualisation des données lorsqu'une nouvelle irrégularité de même nature sera constatée.

Pour rappel, cette finalité est la suivante :

d) le respect des principes et règles d'utilisation des systèmes d'information de la Ville tels que fixés dans la présente Charte.

---

[5] Par anomalie, on entend, notamment :
- L'utilisation simultanée d'un même compte individuel sur plusieurs ordinateurs ou des tentatives d'utilisation d'un compte individuel non propriétaire ou encore des tentatives d'utilisation d'un compte individuel sur un ordinateur non propriétaire ;
- Des connexions longues et/ou fréquentes sur des sites dont l'accès ne peut être justifié d'un point de vue professionnel ou encore des tentatives de connexion à des sites non autorisés ;
- Une fréquence anormale de messages, la présence d'adresses suspectes, la présence et la taille de fichiers joints ;
- Une utilisation excessive des ressources informatiques (saturation de CPU, de disques, de bande passante, …).

Lorsque l'anomalie, l'usage interdit, abusif ou excessif d'un ou de plusieurs comptes utilisateurs, de l'accès à l'internet ou du système de courrier est avéré, la, le ou les utilisatrices, les utilisateurs seront entendus, avec leur supérieur hiérarchique, dans leurs explications, par l'agent, l'agente responsable du contrôle ainsi que le Chef ou la Cheffe de service de celui-ci, de celle-ci.

Le justificatif fourni par l'agent, l'agente sera :

- soit suffisant pour classer dans le répertoire des incidents,
- soit insuffisant et le Chef, la Cheffe de service pourra alors avertir la Directrice générale, laquelle se réserve le droit de recourir aux procédures et sanctions applicables au personnel communal.

La Directrice générale veillera à informer la personne déléguée à la protection des données de toute situation constitutive d'un manquement, d'une contrariété à la réglementation applicable en matière de protection des données à caractère personnel.

Des poursuites pourront également être engagées par la Ville de Namur en cas d'usage interdit ou abusif d'un compte utilisateur, de l'accès à l'internet ou du système de courrier par des utilisateurs, des utilisatrices autres que ses agents et agentes.

3. CONTROLE DE LA TELEPHONIE FIXE ET MOBILE

• LA TELEPHONIE FIXE

En relation avec les frais de communication facturés à la Ville, lesquels sont examinés, le service de Gestion Immobilière peut procéder au contrôle des factures.

Dans le cadre de cet examen, l'identification d'un poste fixe à l'origine d'une anomalie (montant anormal, numéro surtaxé, …) permet d'identifier l'agent ou l'agente titulaire du poste.

L'agente, l'agent, en charge du contrôle qui constate une anomalie avertit sa Cheffe ou son Chef de service, ils évaluent ensemble la situation. Dans ce cadre, un contact peut être pris avec la ou le supérieur hiérarchique de l'agent, de l'agente titulaire du poste litigieux afin de mener les investigations utiles à l'identification de l'auteur des appels (accès au poste, travail à distance, …).

L'agente, l'agent, en charge du contrôle et sa, son supérieur hiérarchique peuvent entendre l'agent ou l'agente titulaire du poste litigieux en présence de la ou du supérieur hiérarchique de celui-ci, de celle-ci.

Un rapport est alors établi par l'agente, l'agent en charge du contrôle et adressé au Chef ou à la Cheffe de service ou en tous cas, à la ou au supérieur hiérarchique de l'agent, de l'agente, titulaire du poste litigieux qui prendra les dispositions qu'elle ou il estime nécessaires dont, notamment, l'information de la Directrice générale.

La Directrice générale se réserve alors le droit de recourir aux procédures et sanctions applicables au personnel communal.

Un contrôle peut également être initié par l'agent, l'agente en charge du contrôle à la demande d'un Chef ou d'une Cheffe de service disposant d'un accord écrit d'un Chef ou d'une Cheffe de département.

Dans l'hypothèse d'une utilisation abusive de la téléphonie fixe à des fins privées, d'appels vers des numéros surtaxés ou à l'international en dehors de toute finalité professionnelle admise, le montant correspondant à ces communications sera refacturé à l'agent, à l'agente.

- LA TELEPHONIE MOBILE

En relation avec les frais de communication facturés à la Ville, lesquels sont examinés, le service de Gestion Immobilière peut procéder au contrôle des factures (sous réserve de la facturation des abonnements de type forfait).

Dans le cadre de cet examen, l'identification d'une consommation à partir d'un numéro attaché à un téléphone portable présentant une anomalie (montant anormal, quantité d'appels vers un ou plusieurs numéros ou fréquents à l'international, numéro surtaxé, …) permet d'identifier l'agent ou l'agente titulaire du numéro.

L'agente, l'agent, en charge du contrôle qui constate une anomalie avertit sa Cheffe ou son Chef de service, ils évaluent ensemble la situation. Dans ce cadre, un contact peut être pris avec la ou le supérieur hiérarchique de l'agent, de l'agente titulaire du numéro litigieux afin de mener les éventuelles investigations utiles à l'identification de l'auteur des appels.

L'agent, l'agente en charge du contrôle et sa, son supérieur hiérarchique peuvent entendre l'agent ou l'agente titulaire du numéro litigieux en présence de la ou du supérieur hiérarchique de celui-ci, de celle-ci.

Un rapport est alors établi par l'agent, l'agente en charge du contrôle et adressé au Chef ou à la Cheffe de service ou en tous cas, à la, au supérieur hiérarchique de l'agent, l'agente titulaire du numéro litigieux qui prendra les dispositions qu'elle ou il estime nécessaires dont, notamment, l'information de la Directrice générale.

La Directrice générale se réserve alors le droit de recourir aux procédures et sanctions applicables au personnel communal.

Un contrôle peut également être initié par l'agent, l'agente en charge du contrôle à la demande d'un Chef ou d'une Cheffe de service disposant d'un accord écrit d'un Chef ou d'une Cheffe de département.

Dans l'hypothèse d'une utilisation abusive de la téléphonie mobile à des fins privées, d'appels vers des numéros surtaxés ou à l'international en dehors de toute finalité professionnelle admise et donc d'appels non renseignés comme privés par le biais des fonctionnalités dédiées, le montant correspondant à ces communications sera refacturé à l'agent, à l'agente.

VII. LES RESPONSABILITÉS ET SANCTIONS ENCOURUES EN CAS DE NON-RESPECT DE LA CHARTE

Le matériel physique, informatique (matériel et logiciel) et de téléphonie sont des outils de travail appartenant à la Ville et mis à disposition des utilisateurs et utilisatrices.

Tout équipement, toute information mis, mise à disposition doit être géré, gérée raisonnablement, comme toute personne prudente et diligente.

Chaque utilisateur, chaque utilisatrice veille à l'intégrité de ses outils de travail et de l'information à laquelle il accède.

Tout un chacun veille à la bonne conduite des activités de la Ville.

Les droits d'accès au système d'information ainsi que les conditions d'utilisation sont accordées à chaque utilisateur, utilisatrice par la Ville de Namur en considération stricte des fonctions qu'il ou elle occupe.

Chaque utilisateur, chaque utilisatrice est responsable de l'usage professionnel, sécurisé et régulier du système d'informations mis à sa disposition dès qu'il y accède, notamment sur base de ses propres identifiants et accès.

L'utilisatrice, l'utilisateur reconnaît être bien informé du fait que le non-respect des dispositions de la présente Charte peut être constitutif d'un manquement aux devoirs professionnels susceptible d'engendrer la mise en œuvre de procédures et de sanctions applicables au personnel communal.

Le non-respect des dispositions de la présente Charte est également susceptible d'engager la responsabilité pénale de l'utilisateur, de l'utilisatrice eu égard, notamment, à l'article 314*bis* du Code pénal (Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique).

La Ville se réserve le droit de réclamer des dommages et intérêts pour tout dommage du au non-respect de la Charte.