MAIRIE DE COTONOU
RÉPUBLIQUE DU BÉNIN

SECRÉTARIAT EXÉCUTIF
03 BP : 1777
Cotonou - BÉNIN
Tél : +229 21 30 95 69
mairiecotonou.infos@gouv.bj
www.cotonou.mairie.bj

MAIRIE DE COTONOU

CHARTE INFORMATIQUE

Contenu

Préambule

La Mairie de Cotonou met en œuvre les systèmes d'informations nécessaires à ses activités. Elle est représentée par le Maire et le Secrétaire Exécutif (loi n° 2021-14 du 20 DECEMBRE 2021 PORTANT CODE DE L'ADMINISTRATION TERRITORIAL EN REPUBLIQUE DU BENIN).

Les agents, dans l'exercice de leurs fonctions, sont amenés à utiliser ces systèmes mis à leur disposition.

Cette charte vise à :

a) sensibiliser les Utilisateurs (agents) sur les risques et conséquences pour l'administration communale et ses responsables en cas d'une utilisation mauvaise, incontrôlée ou non-sécurisée. Il s'agit :

- du piratage des informations ou logiciels de la mairie ;
- des attaques virales ;
- des préjudices à l'image de la commune ;
- des indiscrétions ;
- de la détention ou diffusion de données protégées par la loi ;
- de la consommation exagérée de ressources.

b) informer formellement l'Utilisateur (agent)
c) permettre, dans le cadre de la loi, les contrôles nécessaires de l'usage du poste de travail.

Dans le but d'assurer la transparence à l'égard des Utilisateurs (agents), la promotion d'une utilisation loyale, responsable et sécurisée des systèmes d'information, la présente charte pose les règles relatives à l'utilisation des ressources de gestion, d'information et de communication de la mairie de Cotonou.

1 Champ d'application

1.1 Système d'information et de communication

Les systèmes d'information de la mairie sont notamment constitués des éléments suivants : ordinateurs (fixes ou portables), périphériques, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, services en ligne, fichiers, données et bases de données, système de messagerie, intranet, extranet, le site web de la mairie, les plateformes multimédias, les e-services (services dématérialisés), etc.

Les e-services, à travers les plateformes de la mairie de Cotonou et de l'Etat Central, sont fournis aux usagers/citoyens en vue d'être utilisés uniquement pour des buts professionnels légitimes et en conformité avec les politiques, procédures, directives et instructions en vigueur.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie des systèmes d'information, le matériel personnel des agents connectés aux réseaux de la mairie, ou contenant des informations à caractère professionnel concernant la mairie.

1.2 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des **Utilisateurs** des systèmes d'information de la mairie, quel que soit leur statut, y compris les conseillers locaux et municipaux, le personnel communal, intérimaires, stagiaires, employés de sociétés prestataires ou même des visiteurs occasionnels.

Les Utilisateurs veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder aux systèmes d'information, soit sur l'un des sites de la commune : arrondissements, services déconcentrés, soit à partir de tout lieu de travail déporté, notamment en cas de télétravail.

Chaque agent communal a la responsabilité de protéger la confidentialité des e-ressources (ressources en ligne) de la mairie.

2 Confidentialité des paramètres d'accès

L'accès à certains éléments des systèmes d'information (comme la messagerie professionnelle électronique, l'accès au wifi, les sessions sur les postes de travail, le réseau, certaines applications ou plateformes e-services) est protégé par des paramètres de connexion (identifiants, mots de passe).

Ces paramètres sont personnels à l'Utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des Utilisateurs (agents). Il ne doit pas modifier les paramètres d'accès au réseau (adresses IP…).

Un Utilisateur (agent) ne doit pas s'approprier, modifier ou tenter de décrypter le mot de passe d'un autre Utilisateur.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'Utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.

Lorsqu'ils sont choisis par l'Utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Les mots de passe doivent être conservés de façon strictement confidentielle. Ils ne doivent pas être évidents (pas de surnoms, de noms des enfants, d'initiales ni de mots d'un dictionnaire) et doivent être composés de caractères alpha numériques et de caractères spéciaux. (8 caractères minimum).

L'Utilisateur (agent) ne doit pas utiliser de comptes autres que ceux auxquels il a légitimement accès. L'Utilisateur (agent) ne doit pas masquer son identité par quelque façon que ce soit.

3 Accès aux données

3.1 Sécurisation des accès

La mairie met en place les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle des systèmes d'information. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de code du numérique ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des Utilisateurs (agents).

Les personnes ayant accès à des données confidentielles du fait de leur activité sur la maintenance des e-ressources sont assujetties à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître. A ce titre, elles peuvent effectuer les opérations de sauvegarde et de duplication nécessaires prévues légalement par les textes en vigueur (LOI N° 2017-20 DU 20 AVRIL 2018 PORTANT CODE DU NUMERIQUE EN REPUBLIQUE DU BENIN).

En cas d'absence, même temporaire, il est impératif que l'Utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

Les Utilisateurs doivent toujours activer un économiseur d'écran protégé par mot de passe lorsqu'ils laissent un ordinateur sans surveillance. A la fin de la journée, ils doivent sortir du système et mettre les ordinateurs hors tension avant de s'absenter.

En cas d'accès au système d'information avec du matériel n'appartenant pas à la mairie, l'Utilisateur doit obtenir une autorisation préalable et écrite (ou par mail) du Secrétariat Exécutif (La Direction des Systèmes d'Information).

3.2 Utilisation des matériels

Il appartient à l'Utilisateur (agent) de veiller à la sécurité du matériel utilisé et à son innocuité.

L'Utilisateur (agent) s'engage à prendre soin des matériels informatiques mis à sa disposition. Il informe la Direction des Systèmes d'Information de toute anomalie constatée. Une anomalie peut être l'indice d'une infection par un virus ou d'un autre problème de sécurité.

Le vol ou le détournement d'un ordinateur ou de tout matériel informatique doit être signalé aussi rapidement que possible au supérieur hiérarchique ainsi qu'à la Direction des Systèmes d'Information en fournissant le nom de l'Utilisateur (agent) directement concerné, le modèle du matériel, la nature des informations contenues, la date du vol, une copie de la déclaration à la police le cas échéant ainsi que toutes autres informations pertinentes relatives au vol.

L'Utilisateur doit enregistrer les données sur les serveurs prévus à cet effet, et ne stocker sur un support autre (ordinateurs fixes ou portables, disques durs externes, clés USB...) que le strict nécessaire. Ces fichiers doivent être enregistrés sur les serveurs dès que possible.

L'Utilisateur ne doit pas installer de logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques d'atteinte à la sécurité au sein de la mairie.

L'Utilisateur veille au respect de la confidentialité des informations en sa possession. IL doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de code du numérique, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celles de la mairie ou susceptible de lui causer un quelconque préjudice en utilisant les systèmes d'information de la mairie.

L'Utilisateur ne doit ni lire, ni copier, ni tenter de lire ou copier les fichiers d'un autre Utilisateur sans son autorisation. Il ne doit également ni intercepter, ni tenter d'intercepter les communications privées entre Utilisateurs, qu'elles consistent en courrier électronique, échanges de données sur l'intranet communal.

L'Utilisateur ne doit copier aucun logiciel autre que ceux du domaine public libres de droit. Il ne pourra installer sur son poste de travail que les logiciels et/ou fichiers légalement obtenus ou ceux qui sont libres de tout droit.

L'Utilisateur doit veiller à l'utilisation professionnelle du matériel permettant une

consommation raisonnable des ressources informatiques à disposition.

4 Utilisation d'internet

Dans le cadre de leur activité, les Utilisateurs (agents) ont accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé.

La Direction des Systèmes d'Information est habilitée à imposer des configurations des navigateurs et à restreindre le téléchargement de certains fichiers.

La contribution des Utilisateurs (agents) à des fora de discussion, systèmes de discussion instantanée, blogs, sites extérieurs à l'activité de la mairie est interdite.

Les Utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts ou à l'image de la mairie avec les moyens qu'elle met à leur disposition, y compris sur internet.

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire à l'activité professionnelle au regard des fonctions exercées.

En particulier, l'Utilisateur ne doit pas se connecter, sous peine de dénonciation aux instances judiciaires, sur des sites à caractères pornographiques, pédophiles, mettant en cause des mineurs.

La transmission ou mise à disposition d'informations ou documents professionnels, par le biais d'internet ou de tout moyen de diffusion ou de stockage en ligne, est prohibée si elle ne sert pas directement l'activité professionnelle de l'Utilisateur.

5 Messagerie

5.1 Mise à disposition

Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une **adresse de messagerie électronique professionnelle**.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les agents sont invités à informer la Direction des Systèmes d'Information des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

La transmission d'informations ou documents professionnels par courrier électronique ou messagerie instantanée à des fins ne servant pas directement les activités ou attributions professionnelles de l'Utilisateur (de l'agent) est prohibée.

5.2 Utilisation professionnelle

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir la communication des informations transmises.

L'Utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs.

En cas d'envoi à une pluralité de destinataires, l'Utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leurs adresses électroniques à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

Les Utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de code du numérique et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, racistes, haineux, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Afin d'éviter l'engorgement du système de messagerie, l'Utilisateur doit s'assurer qu'il envoie des pièces avec une taille minimale, et doit utiliser des systèmes alternatifs d'envoi si la ou les pièce(s) jointe(s) est de taille significative et/ou doit être effectué envers un grand nombre de destinataires.

5.3 Utilisation personnelle

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Ils doivent être utilisés dans une quantité suffisamment raisonnable pour ne pas nuire à l'activité professionnelle de l'Utilisateur (de l'agent) ou celle des autres Utilisateurs (agents).

Les messages envoyés doivent être signalés par la mention « Privé » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé ».

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Privé ». En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

6 Contrôle des activités

6.1 Contrôles automatisés

Les systèmes d'information s'appuient 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 des systèmes d'information, en protégeant la sécurité des informations de la mairie, 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 (agents) sont informés que de multiples traitements sont réalisés afin de surveiller les activités des systèmes d'information. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppression 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 web ou le téléchargement de fichiers.

L'attention des Utilisateurs (agents) 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.

6.2 Contrôles manuels

En cas de dysfonctionnement constaté, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs (agents) par **une personne habilitée** par la Direction des Systèmes d'Information (DSI).

Lorsque le contrôle porte sur les fichiers d'un Utilisateur (agent), et sauf risque ou événement particulier, **cette personne habilitée** ne peut ouvrir les fichiers identifiés par l'agent comme fichiers personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé.

7 Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'Utilisateur (agent) et d'entraîner à son

encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie des systèmes d'information, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un Utilisateur (agent), celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

8 Information du personnel communal

La présente charte est communiquée individuellement à chaque agent.

9 Entrée en vigueur

La présente charte est applicable à compter du 1er janvier 2024.