

DÉPARTEMENT DU MORBIHAN
EAU DU MORBIHAN

DATE DE CONVOCATION : 04/05/2023			
Nombre de délégués en exercice	Présents	Absents	Pouvoirs
14	8	5	1

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS
DU BUREAU

L'an deux mille vingt trois, le douze mai, le Bureau de Eau du Morbihan, dûment convoqué, s'est réuni à Vannes, sous la présidence de Monsieur Dominique RIGUIDEL, Président de Eau du Morbihan.

Étaient présents :

Monsieur Vincent COWET. Monsieur Roland GASTINE. Monsieur Tibault GROLLEMUND. Monsieur Didier GUILLOTIN. Monsieur Yannick LE BORGNE. Madame Martine PARE. Monsieur Jérôme REGNIER. Monsieur Dominique RIGUIDEL

Avaient donné pouvoir :

Monsieur Bernard LE BRETON

Étaient excusés :

Monsieur Denis BERTHOLOM. Madame Pascale GILLET. Monsieur Raymond HOUeix. Monsieur Bruno LE BORGNE. Monsieur Benoît ROLLAND

Les présents formant la majorité des membres en exercice, le Bureau peut valablement délibérer.

.../...

B_2023_024A - Adoption de la Charte d'utilisation du système d'information

Vu le Code général des collectivités territoriales ;

Vu la délibération n° CS-2020-045 du Comité Syndical du 25 septembre 2020 portant délégation d'attributions au Bureau ;

Vu l'avis du Comité Social Technique en date du 4 mai 2023 ;

Vu le rapport du Président ;

Le Bureau après en avoir délibéré, décide :

- d'adopter le projet de Charte d'utilisation du système d'information, annexé à la présente délibération ;*
- de charger le Président de l'exécution de la présente décision.*

Fait et délibéré à Vannes, le 12 mai 2023
(au registre suivent les signatures)

Pour extrait certifié conforme
Le Président,



Dominique RIGUIDEL

DÉTAIL DU VOTE

POUR	9
CONTRE	0
ABSTENTION	0
NE PARTICIPE PAS	0

Envoyé en préfecture le 16/05/2023

Reçu en préfecture le 16/05/2023

Affiché le **16/05/2023**

ID : 056-255601072-20230516-B_2023_024A-DE



service public d'eau potable

CHARTRE D'UTILISATION DU SYSTEME D'INFORMATION

Sommaire :

1 Préambule.....	3
1. 1 Définitions	3
1. 2 Application de la charte.....	3
2 Droits d'accès	3
2. 1 Suspension des droits d'accès au système d'information	4
2. 2 Suppression des droits d'accès au système d'information.....	4
3 Sécurité des accès.....	4
4 Devoir d'alerte.....	5
5 Accès à distance au système d'information.....	5
6 Obligations au départ d'un utilisateur ou lors d'un changement d'affectation	5
7 Matériels.....	6
7. 1 Utilisation de matériel et de périphériques personnels	6
8 Logiciels.....	6
9 Messagerie	6
9. 1 Protection de la messagerie contre les virus et le piratage	7
9. 2 Utilisation de la messagerie professionnelle à des fins personnelles.....	7
9. 3 Secret des correspondances	7
10 Accès Internet.....	7
10. 1 Accès aux ressources multimédia	7
10. 2 Utilisation d'internet à des fins personnelles.....	7
11 Réseaux sociaux, forums et blogs	8
11. 1 Accès aux réseaux sociaux dans le cadre professionnel	8
11. 2 Accès aux réseaux sociaux dans la sphère privée	8
12 Fichiers nominatifs et données personnelles.....	8
12. 1 Création des fichiers nominatifs et des données personnelles.....	8
12. 2 Traitement et usage des fichiers nominatifs et des données personnelles.....	8
12. 3 Respect de la loi informatique et libertés et du RGPD	9
13 Secret professionnel et confidentialité	9
14 Propriété intellectuelle et droit d'auteur	9
15 Respect de la vie privée et droit à l'image.....	10
16 Stockage des données.....	10
17 Contrôles techniques	10
18 Accès aux locaux et installations techniques	11
19 Infractions à la loi	11
20 Sanctions.....	11
21 Notification et entrée en vigueur de la charte et de ses actualisations.....	11
22 Consultation du Comité Social Territorial.....	12

1 Préambule

Eau du Morbihan met à disposition des utilisateurs les moyens nécessaires à leurs missions en termes d'accès au système d'information.

La présente charte a pour objectif de définir un code de conduite pour une utilisation responsable du système d'information dans le respect des lois en vigueur et de sensibiliser les utilisateurs aux exigences de sécurité.

L'utilisateur s'engage à utiliser les outils informatiques et de communication mis à sa disposition dans le respect des règles déontologiques, notamment liées au statut de fonctionnaire, ainsi que des lois applicables concernant notamment la vie privée, la collecte et le traitement de données personnelles, les systèmes de traitement automatisé de données, le secret des correspondances, la propriété intellectuelle...

La présente charte, document de référence, a donc pour objet :

- de définir les conditions générales et particulières d'utilisation des ressources informatiques et de communication de Eau du Morbihan,
- de porter à la connaissance de chaque utilisateur les règles d'utilisation des outils mis à sa disposition pour se prémunir d'actions engageant sa responsabilité civile et/ou pénale, et sa responsabilité disciplinaire,
- de porter à la connaissance des utilisateurs les dispositifs mis en place pour garantir la sécurité et la performance des outils mis à leur disposition dans le respect des lois en vigueur,

1. 1 Définitions

Système d'information : désigne toutes les ressources informatiques mises à disposition des élus et du personnel de Eau du Morbihan : logiciels, matériels, réseaux, accès Internet, messagerie, téléphonie...

Utilisateur : désigne l' élu, l'agent quel que soit son statut ou toute autre personne pouvant, dans le cadre de ses fonctions dans les services de la Collectivité, accéder au système d'information de Eau du Morbihan.

Collectivité : désigne l'entité pour laquelle l'utilisateur accède au système d'information (Eau du Morbihan).

RSI : Responsable des systèmes d'information de Eau du Morbihan.

1. 2 Application de la charte

La charte générale s'applique aux agents de la Collectivité.

2 Droits d'accès

Le droit d'accès est ouvert par le RSI sur demande de la hiérarchie de l'utilisateur.

Le droit d'accès est personnel et limité aux autorisations de l'utilisateur. Il cesse avec la disparition des raisons qui ont motivé leur attribution.

La hiérarchie de l'utilisateur doit prévenir le RSI de tout changement de poste, départ, modification des missions pouvant avoir un impact sur les droits d'accès au système d'information.

2. 1 Suspension des droits d'accès au système d'information

Les droits d'accès de l'utilisateur sont suspendus :

- dans le cadre d'une cessation temporaire d'activité (par exemple un arrêt maladie de longue durée),
- dans le cadre de l'exercice du pouvoir de sanction de la collectivité, si un usage illicite ou abusif est suspecté ou prouvé par l'autorité hiérarchique, après en avoir informé l'utilisateur et l'avoir entendu.

2. 2 Suppression des droits d'accès au système d'information

Les droits d'accès de l'utilisateur sont supprimés :

- lors de la cessation définitive de l'activité professionnelle,
- dans le cas d'un changement de service ou d'une mutation.

3 Sécurité des accès

Pour accéder aux ressources, un nom de compte « identifiant » est fourni à l'utilisateur auquel est associé un mot de passe strictement personnel et confidentiel. D'autres moyens d'authentification (code PIN, cartes à puce, clés USB, authentification multi facteurs...) peuvent être mis en œuvre en fonction des outils utilisés (Smartphone, signature électronique, contrôle d'accès...).

Un mot de passe doit être constitué 12 caractères minimum et comporter en termes de complexité des caractères alphanumériques et spéciaux. Il ne doit pas être un mot ou un nom usuel, et doit différer des 5 précédemment utilisés.

Le seuil de verrouillage des comptes est de 5 tentatives d'ouvertures de session.

Les mots de passe utilisés dans la sphère professionnelle doivent être différents des mots de passe utilisés dans la sphère privée.

Pour des raisons de sécurité, un mot de passe doit obligatoirement être changé régulièrement, tous les 90 jours.

Chaque utilisateur est responsable de l'utilisation qui est faite de son compte et de ses droits d'accès. Il lui est strictement interdit de communiquer à un tiers ou de laisser à la vue de tous son mot de passe ou tout autre moyen d'authentification.

A ce titre, toute opération réalisée par recours au moyen propre d'authentification est réputée avoir été effectuée sous la seule et entière responsabilité de son titulaire.

Aussi et afin d'éviter ces difficultés, l'utilisateur s'interdit de laisser son ordinateur sans surveillance. S'il doit s'absenter de son bureau ou s'éloigner de son ordinateur, il s'engage à verrouiller sa session afin qu'un tiers non autorisé ne puisse y avoir accès.

Par ailleurs, la collectivité peut mettre en place un système de verrouillage automatique des ordinateurs inactifs, selon une temporisation qu'elle déterminera.

4 Devoir d'alerte

L'utilisateur est tenu d'avertir immédiatement son supérieur hiérarchique et/ou la DSI :

- de toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation,
- de toute atteinte aux données à caractère personnel,
- de tout dysfonctionnement logique ou technique constaté,
- de la perte ou du vol de matériel,
- de toute anomalie découverte : intrusion, vol ou perte de matériel...,
- de toute violation ou tentative de violation suspectée de ses accès,
- du vol de tout moyen d'authentification,
- de toute intrusion ou tentative d'intrusion dans le système informatique en utilisant un moyen d'authentification lui appartenant,
- et de manière générale de toute anomalie constatée du poste de travail.

5 Accès à distance au système d'information

Les dispositions de la présente charte s'appliquent dans le cas d'un accès à distance au Système d'Information de la Collectivité.

L'utilisation de matériels et périphériques personnels n'est pas autorisée pour un usage professionnel à distance

Les obligations de l'utilisateur sont les mêmes que celles qui s'appliquent sur son lieu de travail notamment :

- ne pas laisser son ordinateur, son Smartphone ou autre matériel sans surveillance,
- ne pas laisser un tiers consulter l'ordinateur, le Smartphone ou autre matériel,
- verrouiller le matériel en cas d'absence,
- fermer toutes sessions ouvertes en cas d'absence,
- ne pas connecter un périphérique non contrôlé par le RSI au préalable,
- ...etc.

6 Obligations au départ d'un utilisateur ou lors d'un changement d'affectation

Au départ de son poste, l'agent, sous la responsabilité de sa hiérarchie, doit :

- restituer le matériel mis à sa disposition,
- supprimer ses documents personnels,
- trier et le cas échéant supprimer ses documents professionnels en accord et sous la responsabilité de sa hiérarchie.

Il est interdit à l'utilisateur de conserver des documents appartenant à son service d'origine, sauf autorisation motivée de sa hiérarchie. L'utilisateur a obligation de garder confidentielles toutes informations ou documents dont il a eu connaissance lorsqu'il était en poste. L'obligation de secret professionnel doit perdurer.

En cas de départ définitif de la Collectivité, l'utilisateur ne peut plus faire l'objet de sanctions disciplinaires mais reste tenu par les obligations légales et pourra, en cas d'irrespect de celles-ci, être poursuivi civilement ou pénalement.

7 Matériels

L'utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquences :

- de modifier le fonctionnement, le paramétrage et les caractéristiques des matériels mis à sa disposition,
- de modifier des éléments de configuration pouvant porter atteinte aux performances des matériels.

7. 1 Utilisation de matériel et de périphériques personnels

La connexion de matériel et de périphériques personnels (tablette, PC portable, clé USB, disque dur, Smartphone...) au réseau de la Collectivité ou au poste de travail professionnel est interdite. Elle peut être autorisée dans le cas d'accès à distance au système d'information ou dans certains cas particuliers, sous réserve d'un contrôle du RSI, notamment du dispositif antivirus et malware.

8 Logiciels

L'utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquences :

- de modifier le fonctionnement, le paramétrage et les caractéristiques des logiciels mis à sa disposition,
 - de modifier des éléments de configuration pouvant porter atteinte aux performances des logiciels.
- L'installation par l'utilisateur de tout logiciel payant ou gratuit est formellement interdite. Dans l'hypothèse où l'utilisateur souhaiterait installer un logiciel payant ou gratuit pour les stricts besoins de son activité professionnelle, il devra au préalable obtenir l'accord écrit du RSI et de son Chef de service.

9 Messagerie

Les échanges et la transmission d'information doivent respecter :

- la présente charte,
- les obligations découlant du statut de fonctionnaire,
- les procédures de validation et de contrôle de chaque collectivité et de chaque direction, en particulier pour tout message qui aurait valeur contractuelle ou d'engagement,
- le secret des correspondances.

9. 1 Protection de la messagerie contre les virus et le piratage

La messagerie est le premier vecteur de propagation des virus et de tentatives de piratage. Un système de protection est mis en place par le RSI et les règles suivantes doivent être respectées par l'utilisateur :

- Il est proscrit de désactiver les systèmes de protection en place,
- les messages suspects (objet ou pièce jointe douteux, émetteur inconnu) ne doivent pas être ouverts et seront transmis au supérieur hiérarchique et au RSI pour analyse. Une fois transmis au RSI, l'utilisateur s'engage à les détruire.

9. 2 Utilisation de la messagerie professionnelle à des fins personnelles

L'utilisation de la messagerie professionnelle à des fins personnelles ou l'accès à une messagerie personnelle sont tolérés dans le cadre d'impératifs de la vie courante et familiale et à la condition que cela n'affecte pas le fonctionnement de la messagerie professionnelle.

9. 3 Secret des correspondances

L'accès aux courriers électroniques privés, émis ou reçus par la messagerie professionnelle est interdit, que ce soit par un supérieur hiérarchique de l'utilisateur ou par un collègue. La violation du secret des correspondances est sanctionnée pénalement. Toutefois, un administrateur peut prendre connaissance de correspondances privées uniquement pour assurer la sécurité du système d'information. Il ne peut en aucun cas les divulguer.

Pour bénéficier du droit au respect de la vie privée et du secret des correspondances, les messages devront comporter la mention « Personnel » dans l'en tête.

10 Accès Internet

10 .1 Accès aux ressources multimédia

L'accès internet à des ressources multimédia mobilise une bande passante importante et risque d'engorger et de ralentir les accès aux réseaux. Il est donc strictement interdit d'accéder à des ressources multimédia sauf pour les besoins de l'activité professionnelle.

10 .2 Utilisation d'internet à des fins personnelles

Une consultation ponctuelle de sites Internet dont le contenu n'est pas contraire à l'ordre public et aux règles éthiques et déontologiques est admise. Elle est possible dans le cadre d'une utilisation raisonnable et en dehors des heures de travail. Elle ne doit pas affecter la sécurité du système d'information ou le bon fonctionnement des services.

Des dispositifs de filtrage de sites non autorisés ont été mis en place par le RSI :

- sites de vente en ligne,
- sites de loisirs,
- sites de jeux,
- sites communautaires,
- sites incitant à la haine,

- sites à caractère pornographique, pédophile,
- sites violents,
- sites faisant l'apologie du terrorisme,
- ...

11 Réseaux sociaux, forums et blogs

11 .1 Accès aux réseaux sociaux dans le cadre professionnel

L'utilisation des réseaux sociaux, forums et blogs doit être limitée à la sphère professionnelle et s'inscrit dans le cadre des obligations découlant du statut de fonctionnaire.

11 .2 Accès aux réseaux sociaux dans la sphère privée

Conformément aux obligations découlant du statut de fonctionnaire, il est interdit à l'utilisateur des réseaux sociaux, forums et blogs, dans le cadre de sa sphère privée, de faire état de son activité professionnelle, d'émettre des opinions liées à son activité professionnelle ou de faire des communications sur ou au nom de la Collectivité.

12 Fichiers nominatifs et données personnelles

12 .1 Création des fichiers nominatifs et des données personnelles

Seules les personnes dûment autorisées par leur hiérarchie peuvent procéder pour le compte de la Collectivité, en qualité de service gestionnaire de données nominatives, à la collecte et au traitement de ces données.

Les personnes non autorisées ne peuvent en aucun cas procéder à la collecte de données personnelles, et ce quelle qu'en soit la finalité.

12 .2 Traitement et usage des fichiers nominatifs et des données personnelles

L'usage de fichiers nominatifs n'est possible que par des personnes autorisées, dans le cadre des missions de la collectivité et pour les finalités déclarées. Tout détournement de finalité est passible de sanctions pénales.

Les personnes concernées doivent préalablement être informées sur la finalité et les destinataires du traitement des informations.

Seules les informations pertinentes et nécessaires doivent être collectées et plus généralement aucune donnée sensible ne peut être collectée comme :

- les opinions politiques, syndicales, philosophiques, religieuses,
- l'origine,
- l'orientation sexuelle,
- l'état de santé,
- l'apparence physique,
- le handicap,

- l'appartenance à une ethnie ou une race,
- ...

La communication de données personnelles n'est possible qu'à l'encontre de personnes autorisées et dans le cadre d'une finalité déclarée.

12 .3 Respect de la loi informatique et libertés et du RGPD

Pour tout traitement de données personnelles, l'utilisateur se conformera au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le RGPD.

L'utilisateur est informé que les données à caractère personnel le concernant sont conservées par le service informatique pendant toute la durée de leur relation contractuelle et des délais en matière de prescription. L'utilisateur est informé qu'il dispose, pour des motifs légitimes admis par l'entité, des droits conformes au RGPD tels que droit d'accès, de rectification, d'opposition, droit à l'effacement, à la portabilité, à la limitation du traitement, relatifs à l'ensemble des informations le concernant.

Eau du Morbihan a désigné un Délégué à la Protection des Données personnelles, le DPO ou DPD.

Le DPO ou DPD a pour mission d'informer, de conseiller et de veiller à la conformité des traitements à la réglementation en matière de données personnelles. Il doit être consulté préalablement à la création d'un traitement (mise en place d'un fichier de données personnelles). Il veille au respect des droits des personnes et peut être sollicité via l'adresse mail suivante : dpo@eaudumorbihan.fr.

13 Secret professionnel et confidentialité

L'utilisateur est tenu au secret professionnel et à la confidentialité au regard du grand nombre d'informations notamment sensibles et nominatives auxquelles il peut avoir accès, par exemple :

- Etat civil,
- Cadastre,
- Facture d'eau,
- ...

14 Propriété intellectuelle et droit d'auteur

Tout document, image, base de données, outil, logiciel mis à disposition ou accessibles aux utilisateurs est protégé par le droit d'auteur. Son utilisation, reproduction, représentation, communication sans autorisation préalable de l'auteur est constitutive d'une violation des droits de celui-ci, susceptible de poursuites civiles et pénales. Sont ainsi répréhensibles par exemple les pratiques suivantes :

- Copie non autorisée d'un logiciel,
- Copie et divulgation d'un document interne,
- Copie sans autorisation de l'auteur de documents trouvés sur Internet pour réaliser des documents professionnels,
- Utilisation, recomposition sans autorisation de l'auteur d'images trouvées sur Internet.

15 Respect de la vie privée et droit à l'image

Il est interdit :

- de capter, d'enregistrer, de retranscrire les propos d'autrui sans son consentement,
- d'intercepter ses communications,
- d'usurper son identité,
- de procéder à la collecte et au traitement de données à caractère personnel sans le consentement de la personne et en communiquant ces données à des tiers non autorisés,
- de capter et de diffuser l'image d'une personne sans son consentement. Tout manquement est sanctionné civilement et pénalement.

16 Stockage des données

Les données sont stockées sur les serveurs de Eau du Morbihan et dans des datacenter tiers pour les services hébergés. L'utilisation d'autres moyens de stockage fait l'objet d'une demande d'avis du RSI.

17 Contrôles techniques

Le RSI est garant du bon fonctionnement du système d'information de la Collectivité. Les conditions de son utilisation peuvent faire l'objet de contrôles pouvant aboutir à des sanctions s'il s'avérait que la présente charte n'était pas respectée.

A ce titre, le RSI doit prendre toutes dispositions nécessaires pour garantir ce bon fonctionnement. Il effectue des contrôles techniques dans le respect de la législation en vigueur et notamment conformément aux règles régissant la protection de la vie privée. L'accès aux données personnelles des utilisateurs par l'administrateur n'est justifié que lorsque le bon fonctionnement des systèmes ne peut être assuré par d'autres moyens moins intrusifs.

Les contrôles techniques sont réalisés :

- pour garantir la sécurité du réseau et du système d'information,
- pour l'analyse et le contrôle de l'utilisation des ressources matérielles, logicielles et de la messagerie professionnelle,
- pour vérifier que l'utilisation du système d'information est conforme aux règles de la présente charte,
- pour déceler les surconsommations, notamment en téléphonie,
- pour s'assurer du respect des lois et règlements dans le cadre de l'utilisation d'Internet,
- pour répondre aux requêtes des autorités compétentes.

Les outils de contrôle mis en œuvre par le RSI permettent d'enregistrer les informations suivantes :

- les connexions au réseau : identifiants, dates et heures de connexion,
- les fichiers stockés sur les serveurs : format, date, taille,
- l'inventaire des logiciels installés sur les matériels,
- la taille et le nombre de messages échangés,

- les connexions internet : identifiant de connexion, sites visités, volumes de données transférées, dates et heures de connexion,
- le relevé synthétique des consommations de téléphonie, l'état détaillé des consommations du poste avec masquage des quatre derniers chiffres des numéros appelés et alertes en cas de surconsommation en téléphonie.

Les traitements de données nominatives font l'objet d'une inscription au registre des traitements mis à jour dans le logiciel de catalogage et de suivi des données RGPD.

18 Accès aux locaux et installations techniques

L'accès aux locaux et aux installations techniques placés sous la responsabilité du RSI est interdit aux personnes non autorisées.

Les personnes autorisées ne doivent en aucun cas communiquer ou donner leur moyen d'accès à quiconque (code, clé, etc...) et ce quelle qu'en soit la raison.

19 Infractions à la loi

Certains usages ou manipulations frauduleux sont susceptibles de constituer et de caractériser une infraction à la loi et peuvent entraîner des poursuites civiles et pénales. L'utilisateur a obligation de dénoncer tout crime ou délit dont il aurait connaissance à son supérieur hiérarchique et au RSI pour que ces derniers en avisent le procureur de la République.

Quelques exemples d'infractions :

- une utilisation des moyens portant incitation à la pédophilie, à la haine raciale, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants,
- une utilisation des moyens portant diffamation, injure ou atteinte à la vie privée, à la dignité humaine, à l'ordre public, aux bonnes mœurs ou encore à la sûreté nationale,
- la reproduction, représentation ou diffusion d'une œuvre en violation des droits de l'auteur/et ou du titulaire des droits de propriété intellectuelle,
- la copie de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle,
- la contrefaçon, notamment par fourniture de moyens illicites de piratage informatique...

20 Sanctions

L'accès au système d'information de la collectivité est soumis au respect de la loi, des textes réglementaires et des obligations découlant du statut de fonctionnaire.

En cas de non-respect de la présente charte, l'utilisateur s'expose à des sanctions disciplinaires mais également à des poursuites civiles et pénales.

21 Notification et entrée en vigueur de la charte et de ses actualisations

La présente charte et ses actualisations sont notifiées à chaque utilisateur. Elle entre en vigueur et est opposable dès sa notification

22 Consultation du Comité Social Territorial

Le Comité Social Territorial sera consulté sur les termes de la présente charte le 04/05/2023

Notification à l'agent :

Date de la notification :

Signature :