USESA
Eau Sud de l'Aisne

CHARTE INFORMATIQUE

Dates	Actions	Observations
08/07/2025	Mise en place	

Table des matières

I. Préambule

Cette charte est avant tout un code de bonne conduite et intègre la mise en place du Règlement Général de Protection des Données « RGPD ».

Elle a pour objet de préciser la responsabilité des utilisateurs, en conformité avec la législation, afin d'instaurer un bon usage des ressources informatiques et des services Internet, quel que soit le lieu de travail, y compris en télétravail.

Elle a également pour l'objet de sensibiliser les utilisations aux risques liées à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite.

La prudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de la collectivité.

Elle est portée à connaissance de tout agent concerné.

Pour rappel, l'USESA est soumise au respect de la loi Informatique & Libertés n° 78-17 du 6 janvier 1978 modifiée.

II. Fondements législatifs

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- le Règlement UE 2016/679 dit Règlement général sur la protection des données (RGPD).
- la loi du 20 juin 2018 relative à la protection des données personnelles : cf. http://www.cnil.fr ;
- la législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal) : http://www.legifrance.gouv.fr ;
- la législation relative à la propriété intellectuelle : http://www.legifrance.gouv.fr ;
- la loi du 04/08/1994 relative à l'emploi de la langue française : http://www.culture.fr/culture/dglf ;

III. Définitions

On désignera l'USESA sous le terme « collectivité ».

On désignera de façon générale sous le terme « ressources informatiques », les moyens informatiques de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par la collectivité.

On désignera par « services Internet », la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : TeamViewer, VPN, etc...

On désignera sous le terme « utilisateur », les personnes ayant accès ou utilisant les ressources informatiques et services Internet.

IV. Application

La présente charte s'applique à l'ensemble des agents de la collectivité tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires (prestataires), utilisant les moyens informatiques de la collectivité ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré.

Elle s'applique à toutes les nouvelles technologies d'information et de communication mises à disposition des agents par la collectivité (ordinateur portable, accès internet, PC, smartphone, etc...)

Elle sera annexée, à titre d'information, aux contrats de travail conclus avec les agents contractuels qui auront accès au système informatique de la collectivité.

V. Accès aux ressources informatiques et services internet

A. Les postes informatiques

- Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition de chaque utilisateur :
  - Matériel : PC portable, unité centrale, station d'accueil, écran, clavier, souris...,
  - Système d'exploitation : Windows ...,
  - Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats.

- Toute installation de logiciel doit être faite par le prestataire informatique par le biais du responsable informatique de la collectivité.

- En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches « Windows + L »).

- En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller son PC.

- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel et éteindre son écran.

- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (deux fois par an). Ces mots de passe sont communiqués au responsable informatique. Un minimum de 12 caractères contenant des majuscules, des minuscules, des chiffres et des caractères spéciaux

- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations. Les sauvegardes sont réalisées via les serveurs Cloud et local de la collectivité

- L'utilisateur doit signaler tous dysfonctionnements ou anomalies en saisissant le référent informatique de la collectivité directement et par mail.

- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire.

- Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable et ne doivent être utilisées qu'à des fins professionnelles.

B. La messagerie

- L'utilisation de la messagerie est réservée à des fins professionnelles.

- L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect.

- Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'Autorité Territoriale ou le référent informatique (même en l'absence de l'utilisateur). Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel et confidentiel » dans leur objet. Ces derniers ne pourront alors être ouverts par l'Autorité territoriale ou le référent informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la Loi.

- L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

- L'utilisateur signera tout courriel professionnel.

- L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.

- L'utilisateur doit vérifier le contenu et l'historique des messages transférés (gestion du "Répondre à tous").

- L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

- En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue en dirigeant les expéditeurs vers la boite contact.eau@usesa.fr.
  Un agent du service doit pouvoir gérer les messages pendant son absence.

- La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées par la collectivité.

- Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (ordonnance n° 2005-1516 du 8 décembre 2005). Ils doivent, en conséquence être traités dans les mêmes délais.

- L'utilisateur devra impérativement répondre aux mails reçus sur la boite mail générique par le biais de la boite mail générique. La signature de l'auteur sera ajoutée par l'utilisateur qui gère la boite mail générique.

Les agents ne doivent pas transmettre ou répondre aux messages non professionnels, harcèlement ou de chaînes de lettres : ces messages devront être effacés si vous en recevez après consultation du responsable informatique.

Souvenez-vous que tous les messages que vous envoyez peuvent être transmis sans que vous en ayez connaissance. Ne supposez pas que votre destinataire respecte la confidentialité de votre message.

C. Les sites internet

- L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

- Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

- L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédo-pornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).

- Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

- Le stockage permanent sur les postes de données téléchargées sur Internet est interdit.

- Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

- Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'Autorité territoriale.

- Pour éviter les abus, l'Autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités (Cass. soc. 9 juillet 2008 n° 06-45-800).

- Toute saisie d'informations sur un site Internet professionnel nécessite l'autorisation préalable de l'Autorité territoriale.

- Toute procédure d'achats personnels sur Internet est formellement interdite.

- L'utilisation de forums de discussion est autorisée pour un usage professionnel.

D. Le téléphone

- L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle.

- L'utilisation des téléphones portables personnels doit rester, limitée, occasionnelle et discrète (appels et sms).

- L'Autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.

- En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique.

- L'agent qui quitte définitivement la collectivité doit restituer le matériel qui lui a été confié pour l'exercice de ces missions. Un bon de remise de matériel précisant le modèle, les accessoires annexes et l'état de l'outil mis à disposition est signé par chaque agent de la collectivité

- L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

E. Les identifiants et mots de passe

La plupart des services, qu'ils soient professionnels ou publics, requièrent une authentification.

Les utilisateurs doivent respecter les règles suivantes :

- Les moyens d'authentification (identifiant/mot de passe, certificat/code pin, adresse de messagerie ou autres) fournis par l'administration sont strictement personnels, confidentiels et incessibles ;

- Les mots de passe choisis doivent être suffisamment robustes (combinaison de 12 caractères comprenant lettres en minuscules, majuscules, chiffres, caractères spéciaux, absents du dictionnaire et sans lien évident avec l'utilisateur) ;

- Ils doivent être modifiés régulièrement ;
- Les moyens d'authentification professionnels doivent être utilisés pour des usages uniquement professionnels ;
- Les mots de passe à usage privé ne doivent pas être utilisés dans le cadre professionnel et réciproquement ;

La collectivité peut mettre à la disposition des utilisateurs un « coffrefort logiciel » de gestion des mots de passe pour aider à leur mémorisation. Ce dictionnaire doit rester strictement professionnel.

D'une manière générale, Il appartient à l'utilisateur de veiller à la sécurité et à l'état du matériel utilisé. L'utilisateur s'engage à prendre soin du matériel informatiques mis à sa disposition.

Il informe le responsable informatique 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 doivent être signalés aussi rapidement que possible à son supérieur hiérarchique en fournissant 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'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

La collectivité pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : filtrage d'accès sécurisé, etc...

L'utilisateur est averti que le service informatique a les moyens de contrôler l'activité Internet de chaque poste.

VI. Gestion des impressions et scans.

A. Les impressions

La collectivité met à disposition des utilisateurs un système de contrôle manuel pour récupérer les impressions.

Les utilisateurs devront physiquement s'authentifier avec un code secret afin de récupérer leurs documents et d'en lancer l'impression.

Les impressions doivent se faire en noir et blanc dans la plupart des cas hormis besoin spécifiques définis par le responsable hiérarchique direct de l'utilisateur.

Les mots de passe seront renouvelés régulièrement.

B. Les scans

Chaque utilisateur de la collectivité bénéficie d'un dossier scan propre à sa session et protégé par un mot de passe afin d'assurer la confidentialité des documents numérisés.

VII. Cas du télétravail

Obligation du télétravailleur :

➢ Sécurisez votre connexion internet :

Assurez-vous du bon paramétrage de votre box Internet. Vérifiez son mot de passe d'accès administrateur, changez-le s'il est faible et mettez à jour son logiciel interne. Le site web de votre opérateur (par exemple celui de Bouygues, SFR, Orange et Free), vous accompagnera dans la bonne mise en œuvre de ces étapes.

Si vous utilisez le Wi-Fi, activez l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe (l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande par exemple une vingtaine de caractères). Désactivez la fonction WPS et supprimez le Wi-Fi invité. Ne vous connectez qu'à des réseaux de confiance et évitez les accès partagés avec des tiers.

Ne faites pas en télétravail ce que vous ne feriez pas au bureau. Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels, notamment sur votre navigation web, en veillant à bien séparer les usages professionnels et les usages personnels. Vous pouvez par exemple créer des comptes distincts si vous utilisez une même application pour ces deux sphères.

➢ Restitution de l'ordinateur professionnel lors d'un arrêt maladie :

L'agent en arrêt maladie doit restituer à la collectivité son ordinateur de fonction ainsi que toutes les informations indispensables à la bonne marche de celle-ci, y compris les mots de passe indispensables au bon fonctionnement.

➢ Restitution du matériel utilisé uniquement en télétravail :

En cas de fin de période de télétravail, l'agent doit restituer à son employeur le matériel mis à disposition hormis ce qui lui est nécessaire pour exercer sa mission en présentiel.

VIII. Système de journalisation

La journalisation est gérée par le logiciel ESET Endpoint Security et permet d'enregistrer tous les évènements importants dans un fichier journal, consultable directement depuis l'interface de celui-ci.

Les fichiers journaux peuvent être utilisés pour détecter les erreurs et révéler les intrusions sur votre système. Les journaux du pare-feu ESET contiennent les données suivantes :

- Heure – Date et heure de l'événement.
- Evènement – Nom de l'événement.
- Source – Adresse réseau source.
- Cible – Adresse réseau cible.
- Protocole – Protocole de communication réseau.
- Nom de la règle/du ver – Règle appliquée ou nom du ver, s'il est identifié.
- Application – Application concernée.
- Utilisateur – Nom de l'utilisateur connecté au moment où l'infiltration a été détectée.

Une analyse approfondie de ces données peut aider à détecter les tentatives de compromission de la sécurité du système. De nombreux autres facteurs indiquent des risques potentiels pour la sécurité et permettent d'en minimiser l'impact. Parmi les indicateurs de menace potentielle, on peut citer les connexions fréquentes depuis des emplacements inconnus, les tentatives multiples d'établissement de connexions, la communication d'applications inconnues ou l'utilisation de numéros de port inhabituels.

IX. Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de sa collectivité.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier :

- Il doit appliquer les recommandations de sécurité de la collectivité,
- Il doit assurer la protection de ses informations et il est responsable des droits qui lui sont octroyés par la collectivité, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition,
- Il doit signaler toute tentative de violation de son ordinateur ou compte et, de façon générale, toute anomalie qu'il peut constater,
- Il doit suivre les règles en vigueur au sein de la collectivité pour toute installation de logiciel en passant par le responsable informatique,
- Il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers hormis au responsable informatique,
- Il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien,

- Il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers qui ne sont pas en lien avec les missions qu'il exerce,
- Il ne doit pas quitter son poste de travail sans se déconnecter en laissant des ressources ou services accessibles.

X. Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le responsable informatique et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui- même.

XI. Respect de la législation concernant les logiciels

Il est strictement interdit d'effectuer des copies 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. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable informatique.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

XII. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques... Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du responsable informatique de la collectivité et dans le strict respect des règles qui auront alors été définies.

XIII. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

XIV. Le droit à la déconnexion

Le droit à la déconnexion s'entend comme le droit pour tout agent public de ne pas être connecté à un outil numérique professionnel en dehors de son temps de travail.

Ce droit, qui s'inscrit dans une démarche d'amélioration des conditions de travail et d'une meilleure conciliation entre la vie professionnelle et la vie personnelle, a pour objectif le respect des temps de repos et de congés.

Ainsi, ce droit permet aux agents publics de ne pas répondre aux sollicitations professionnelles en dehors des horaires de travail sans risque d'être sanctionnés.

Les règles suivantes peuvent être adoptées :

- Respecter un temps de déconnexion aux outils numériques professionnels d'au moins 11 heures entre 2 journées de travail.
- Respecter les périodes de repos, congés et disponibilité de l'ensemble des agents, périodes pendant lesquelles ils ne sont pas tenus de consulter leurs messages et de répondre aux sollicitations (à l'exception des agents en astreinte).
- En tout état de cause, les responsables de service doivent s'abstenir de contacter leurs agents en dehors de leurs horaires de travail habituels, ainsi que pendant leurs congés ou en cas d'arrêt maladie, sauf nécessité de service ou urgence caractérisée (à définir avec les agents).
- Dans tous les cas, l'usage de la messagerie électronique, du téléphone professionnel ou de tout autre outil numérique en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

XV. Gestion des équipements obsolètes

Pour la gestion des déchets d'équipements électriques et électroniques/matériels informatiques (ordinateurs, téléphone, supports amovibles de sauvegarde, copieurs...) en fin de vie :

- Les matériels informatiques en fin de vie doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations ou toute autre personne.
- Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de type "bas niveau" destiné à effacer les données qui peuvent y être stockées.

- Les téléphones portables doivent être réinitialiser et vider de tous fichiers (documents de travail, photo, coordonnées, etc...) avant cession ou destruction.

Lorsque ces opérations sont confiées à un prestataire, une attestation de bonne réalisation de l'opération de reconditionnement ou de destruction devra être demandée.

Toutes ces opérations sont réalisées sous la surveillance du responsable informatique de la collectivité.

XVI. Sanctions

L'utilisation abusive des ressources informatiques de la part des agents pourra faire l'objet de sanctions administratives.

L'accès aux ressources informatiques et aux services Internet pourra être interrompu sans avis préalable afin de préserver l'intégrité de la collectivité.

En cas de manquement aux obligations imposées par le RGPD, les collectivités et établissements publics concernés peuvent se voir infliger une amende pouvant atteindre 20 millions d'euros pour les entités les plus importantes.

La CNIL pourra émettre des réponses en cas de violation de la réglementation comme des mises en demeure ou des avertissements.

Le Président,

Hugues DAZARD.

Le 08/7/2025

UNION DES SERVICES D'EAU DU SUD DE L'AISNE U.S.E.S.A

RECEPISSE CHARTE INFORMATIQUE

Je soussigné,

Nom :

Prénom :

Service :

Fonction :

Utilisateur des moyens informatiques et réseaux de la collectivité, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à..... Le

Signature

Fait en deux exemplaires :

- **un pour l'intéressé (agent – élu)**
- **un pour la collectivité**

Les informations recueillies sur ce formulaire font l'objet d'un traitement informatisé par le Président de l'USESA sis à 4, Bis avenue Gustave Eiffel – 02400 CHATEAU-THIERRY pour le suivi du caractère opposable de la charte informatique. Le responsable de traitement a désigné l'ADICO sise à Beauvais (60000), 5 rue Jean Monnet en qualité de déléguée à la protection des données. Le traitement est nécessaire au respect de l'intérêt légitime auquel le syndicat est soumis. Les données collectées seront communiquées aux seuls destinataires suivants : USESA. Les données sont conservées pendant la durée de conservation des données prévue par le responsable du traitement, en concordance avec la Durée d'Utilité Administrative.

Vous pouvez accéder aux données vous concernant, les rectifier ou exercer votre droit à la limitation du traitement. Vous disposez également d'un droit d'opposition. Le droit à la portabilité ne s'applique pas dans ce cas. Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez contacter notre délégué à la protection des données ou le service chargé de l'exercice de ces droits à l'adresse suivante : ADICO sise à Beauvais (60000). Si vous estimez que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL. Consultez le site cnil.fr pour plus d'informations sur vos droits.