



# CHARTRE D'USAGE ET DE SÉCURITÉ POUR LES UTILISATEURS DU SYSTÈME D'INFORMATION DE LA MÉTROPOLE **aix-marseille-provence**

—  
Pôle Numérique

Adoptée en Conseil de Métropole le 12 octobre 2023

# Edito

## du Directeur Général des Services

### CHARTE D'USAGE ET DE SÉCURITÉ POUR LES UTILISATEURS DU SYSTÈME D'INFORMATION DE LA MÉTROPOLE AIX-MARSEILLE-PROVENCE

La Métropole Aix-Marseille-Provence encadre depuis 2019 l'usage et la sécurité pour les utilisateurs de son système d'information au moyen d'une charte.

Nous avons tous pris conscience au travers des dernières crises sanitaires et cyber que nous avons traversées ensemble, de l'impérieuse nécessité de garantir la disponibilité et la sécurité de nos outils numériques. Au-delà du contexte actuel, ces outils s'inscrivent de plus en plus au quotidien comme un des éléments essentiels de la continuité et de l'efficacité des services publics.

De plus, les dernières évolutions dans les domaines de l'Intelligence Artificielle (IA), désormais accessibles au plus grand nombre doivent nous interroger sur nos pratiques, les moyens que nous mobilisons et le cadre de confiance que nous devons développer au service de nos usagers.

Par ailleurs, si nos outils numériques occupent une importance de plus en plus grande dans notre activité, il est nécessaire de tenir compte de leur impact sur l'environnement. Notre engagement collectif est de prendre la mesure de l'impact de nos usages et d'adapter individuellement nos comportements pour réduire l'empreinte du numérique.

Nos logiciels, applications mais aussi les données que nous manipulons s'inscrivent dans une croissance continue, toujours au service de notre performance mais surtout dans la perspective du Service Public.

Dans ce contexte, la charte informatique qui encadre notre usage individuel et collectif de ces outils, doit être adaptée pour tenir compte des nouveaux enjeux portés par les technologies de l'IA et l'extension des services que nous développons mais aussi des données que nous manipulons.

J'ai souhaité que la charte informatique soit adaptée pour garantir la pérennité de notre Système d'Information, sécuriser nos usages. Ces adaptations doivent continuer de préserver l'équilibre entre vie privée et professionnelle.

Je vous engage à adopter les bons réflexes dont les grands principes sont rappelés dans cette charte. Je sais compter sur votre engagement mais aussi votre vigilance dans l'usage de ces outils.

**Le Directeur Général des Services,  
Domnin RAUSCHER**

# Table des matières

<b>1. PRINCIPES GÉNÉRAUX .....</b>	<b>4</b>
1.1. Mes obligations en tant qu'utilisateur des outils informatiques de la Métropole.....	5
1.2. Je ne « pirate pas ».....	5
1.3. Protection des données personnelles .....	5
1.3.1. Définitions.....	6
1.3.2. Secret professionnel.....	6
1.4. En cas de manquement à ces règles je m'expose à des risques .....	6
1.5. Le droit à la déconnexion.....	6
1.6. Mes droits sur les données à caractère personnel me concernant.....	6
<b>2. A SAVOIR.....</b>	<b>7</b>
2.1. J'arrive à la Métropole.....	8
2.2. Mes équipements informatiques et télécoms.....	8
2.3. Mes autorisations d'accès sont liées à mon emploi .....	8
2.4. Je suis responsable de l'utilisation des moyens de communication .....	8
2.5. Mon utilisation est professionnelle.....	8
2.6. Ma liberté et celle des autres est protégée.....	8
2.7. Les équipements personnels.....	9
2.8. Usage sobre des outils numériques .....	9
<b>3. INTERNET.....</b>	<b>10</b>
3.1. Je me comporte comme un « surfeur » averti.....	10
3.2. Téléchargements : attention ! .....	10
3.3. Filtrage Internet .....	10
3.4. Qu'en est-il de ma navigation Internet ?.....	11
3.5. Usage de l'Intelligence Artificielle .....	11
<b>4. OUTILS COLLABORATIFS .....</b>	<b>13</b>
4.1. La messagerie .....	14
4.1.1. J'utilise la messagerie à des fins professionnelles.....	14
4.1.2. J'évite les messages trop volumineux .....	14
4.1.3. Concernant les courriels, je reste prudent et professionnel .....	14
4.2. Partage de documents.....	15
4.3. Propriété des données .....	15
<b>5. BUREAUTIQUE .....</b>	<b>16</b>
5.1. La sécurité, ça me concerne aussi .....	17
5.2. Que dois-je faire pour éviter les virus ? .....	17
5.3. Mon utilisation peut être tracée.....	17
5.4. Utilisation des fichiers .....	18
5.5. Perte ou vol de matériel informatique .....	18
<b>6. TELEPHONIE.....</b>	<b>19</b>
6.1. Je maîtrise mon temps de communication.....	20
6.2. Si je suis doté d'un téléphone mobile professionnel .....	20
6.3. Qu'en est-il de ma consommation téléphonique ?.....	20
<b>7. JE QUITTE LA METROPOLE .....</b>	<b>21</b>
7.1. Messagerie .....	22
7.2. Bureautique.....	22
7.3. Téléphonie .....	22
<b>8. contact.....</b>	<b>23</b>

# 1. PRINCIPES GÉNÉRAUX



# 1. PRINCIPES GÉNÉRAUX

**LA PRESENTE CHARTE SE VEUT UN OUTIL PEDAGOGIQUE AU SERVICE DE TOUS LES UTILISATEURS DU SYSTEME D'INFORMATION : INTERNES (ELUS, FONCTIONNAIRES, CONTRACTUELS, APPRENTIS, STAGIAIRES, ...) ET EXTERNES (PRESTATAIRES, PARTENAIRES OU DELEGATAIRES). ELLE VISE A AMELIORER LES COMPORTEMENTS ET DIMINUER LES RISQUES.**

Le respect de la charte est également un engagement individuel à adopter les bonnes pratiques.

Celle-ci ne me dispense pas du respect des réglementations existantes ou à venir.

Les règles de la présente charte s'appliquent quelle que soit ma situation de travail : dans les locaux de la Métropole, en situation de mobilité ou en situation de télétravail.

## 1.1. Mes obligations en tant qu'utilisateur des outils informatiques de la Métropole

Dans mon utilisation des outils informatiques, j'agis avec impartialité, intégrité et probité. Je suis tenu à l'obligation de neutralité et au respect du principe de laïcité.

A ce titre, je m'abstiens notamment de manifester, dans l'exercice de mes missions, mes opinions. Je traite de façon égale toutes les personnes et respecte leur liberté de conscience et leur dignité.

Mes écrits ne recèlent aucune intention violente ou ayant un caractère de discrimination, de harcèlement moral ou sexuel ou d'agissements sexistes. Si je suis destinataire de tels messages, et que je m'estime victime de ces agissements, j'ai la possibilité de le signaler à la Commission de Recueil des Signalements de la Métropole.

Je dois faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont j'ai connaissance dans le cadre de l'utilisation du Système d'Information (cf. 1.3.2).

La sécurité du Système d'Information doit être une préoccupation permanente. Par mes usages, j'en suis le premier acteur et je me comporte en utilisateur averti.

Le Pôle Numérique (PNUM) est garant du bon fonctionnement et de la sécurité du Système d'Information. Je me conforme à ses directives en toutes circonstances.

Ma responsabilité est engagée en cas d'utilisation inappropriée des outils mis à ma disposition et peut entraîner des sanctions.

## 1.2. Je ne « pirate pas »

Les logiciels sont des œuvres intellectuelles couvertes par une législation stricte.

Ainsi la copie privée est interdite. La Métropole ne saurait être tenue pour responsable de l'installation par un utilisateur d'un logiciel dont elle n'a pas acquis les droits. Si je diffuse sur Internet ou si je récupère des images, vidéos, photos ou sons sans le consentement de leur auteur, je suis également en infraction.

Les données circulant sur Internet peuvent être réglementées en termes d'utilisation ou être protégées par un droit de propriété intellectuelle ; je suis responsable de l'utilisation des données que je consulte et que je transfère et je dois notamment m'assurer qu'elles disposent de toutes les autorisations nécessaires pour le faire (licences d'utilisation, droit de reproduction des images, textes et sons ou vidéos).

## 1.3. Protection des données personnelles

### 1.3.1. Définitions

Le règlement européen de protection des données personnelles (RGPD) du 27 avril 2016 et la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définissent les conditions dans lesquelles des données à caractère personnel peuvent être susceptible d'un traitement.

Au sens de ces textes :

- une donnée à caractère personnel est constituée par toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

- un traitement représente toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquée 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.

A titre d'exemple, constituent des traitements de données à caractère personnel :

- Le classement et le traitement de dossiers papier de demande de subventions,
- La constitution d'une base de données de contacts professionnels (mailing list d'entreprises),
- La mise en œuvre d'un système de billettique de transport ou de piscines,
- La géolocalisation des véhicules de collecte,
- Les enquêtes sur les ménages,
- La gestion du personnel ou de la paye.

### 1.3.2. Secret professionnel

En tant qu'agent de la Métropole, je suis tenu au secret professionnel et à la confidentialité au regard du grand nombre d'informations notamment sensibles et nominatives auxquelles je peux avoir accès.

Je m'engage, dans le respect de la déclaration faite dans le registre des traitements (RGPD), à :

- Ne pas utiliser les données à caractère personnel à des fins autres que celles prévues par mes attributions ;
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf si c'est nécessaire à l'exécution de mes fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- M'assurer dans la limite de mes attributions, que seuls des moyens de communications sécurisés seront utilisés pour transférer ces données.

### 1.4. En cas de manquement à ces règles je m'expose à des risques

Si je ne respecte pas les dispositions des présentes règles je pourrais voir mes droits d'accès restreints ou suspendus et, le cas échéant, être passible de sanctions administratives et/ou de poursuites civiles ou pénales.

### 1.5. Le droit à la déconnexion

En tant qu'agent de la métropole, je dispose d'un « droit à la déconnexion », c'est-à-dire de la possibilité de ne pas me connecter aux outils numériques de la Métropole (outils collaboratifs, applications métier) et de ne pas être contacté par mon employeur en-dehors de mon temps de travail (téléphone, courriel).

Ce droit s'exerce en dehors des heures correspondant à ma formule de travail hebdomadaire, définie avec ma hiérarchie.

Si j'estime que ce droit n'est pas respecté, j'évoque en premier lieu la situation avec ma hiérarchie et si le problème persiste, je suis en mesure de saisir la Commission de Recueil des Signalements de la Métropole.

La Métropole trace tous les accès au système d'information à des fins de sécurité, de statistique et de maintenance. Lorsqu'un poste de travail accède au système d'information de la métropole, les données suivantes sont enregistrées :

- L'identifiant de l'utilisateur,
- La date et l'heure de connexion,
- L'adresse IP et le nom du poste de travail,
- Les applications auxquelles il est accédé,
- Le nombre de sessions ouvertes par l'utilisateur,
- La durée totale de l'activité de l'utilisateur.

### 1.6. Mes droits sur les données à caractère personnel me concernant

La Métropole, qui est mon employeur, collecte et traite des données à caractère personnel me concernant.

Je dispose, dans certaines conditions, de droits sur ces données à caractère personnel : accès, rectification, effacement, limitation, portabilité et opposition.

Pour tout renseignement sur les modalités d'exercice de ces droits, je peux saisir le délégué à la protection des données (DPO – Data Protection Officer) de la Métropole (dpo@ampmetropole.fr).

Je peux également introduire une réclamation auprès de la CNIL (www.cnil.fr).

#### À RETENIR

- **Ma correspondance m'engage et engage la Métropole.**
- **Je ne peux pas créer un fichier qui contient des données à caractère personnel même pour un usage interne sans déclaration préalable auprès du DPO.**
- **Je ne télécharge pas de films, de séries TV ou de musiques.**
- **Le Pôle Numérique peut à tout moment modifier mes droits d'accès au Système d'Information.**

## 2. À SAVOIR

## 2. À SAVOIR

### 2.1. J'arrive à la Métropole

Je fais le point sur mes besoins avec ma hiérarchie, qui les transmet au Pôle Numérique pour formaliser mes demandes et dotations en équipement informatique et de télécommunication.

### 2.2. Mes équipements informatiques et télécoms

L'attribution de moyens de communication ou d'outils informatiques dépend de ma fonction et de mes missions. Ces moyens (ordinateur de bureau, PC portable, tablette, téléphone fixe, mobile intelligent, ...) évoluent avec le temps et les technologies.

Je suis personnellement responsable de ces équipements et de leur restitution. Leur usage est professionnel ; il doit rester conforme aux règles définies par l'administration.

Je suis responsable de l'usage des ressources informatiques et du réseau auxquels j'ai accès.

Je dois être raisonnable dans l'utilisation de ces ressources afin d'éviter la saturation ou le détournement à des fins non professionnelles.

Les matériels informatiques et téléphoniques qui me sont confiés sont fragiles, je dois prendre soin d'eux.

### 2.3. Mes autorisations d'accès sont liées à mon emploi

Les autorisations d'accès qui me sont données sont personnelles et incessibles. Elles correspondent au métier qui est le mien et aux fonctions que j'exerce. Elles sont limitées à des activités professionnelles.

Je suis responsable de l'utilisation qui est faite de mon compte d'accès au réseau et aux ressources informatiques, il m'appartient et je ne communique mon mot de passe à aucune tierce personne.

### 2.4. Je suis responsable de l'utilisation des moyens de communication

Je suis personnellement responsable de l'utilisation des ressources informatiques et de télécommunications de la Métropole. Je dois donc, à mon niveau, contribuer à la sécurité du Système d'Information et ne pas effectuer d'opérations pouvant nuire à son bon fonctionnement ainsi qu'à son intégrité.

### JE SUIS RESPONSABLE DE MES IDENTIFIANTS.

### 2.5. Mon utilisation est professionnelle

L'utilisation des équipements informatiques et téléphoniques de l'établissement public est limitée à un usage professionnel. L'utilisation à titre privé est tolérée, mais doit demeurer très occasionnelle et ne doit pas être en contradiction avec les principes déontologiques rappelés dans cette charte.

### 2.6. Ma liberté et celle des autres est protégée

**DES MESSAGES DE NATURE DISCRIMINATOIRE, DIFFAMATOIRE, PEDOPHILE OU D'INCITATION A LA VIOLENCE OU LA HAINE RACIALE DIFFUSES PAR INTERNET OU INTRANET ENGAGENT MA RESPONSABILITE PENALE.**

Le téléphone et la messagerie sont des outils personnels. Ils sont couverts par le secret de la correspondance et protégés par la loi.

Je ne dois pas tenter de lire ou copier les fichiers, les messages d'un autre utilisateur sans son autorisation expresse. Je dois également m'abstenir de toute tentative d'interception sans autorisation des communications entre utilisateurs, qu'elles se composent de messages vocaux ou de courriers électroniques.

## 2.7. Les équipements personnels

### **POUR DES RAISONS DE SECURITE DU SYSTEME D'INFORMATION, LA METROPOLE PROSCRIT TOUT TYPE D'EQUIPEMENT PERSONNEL SUR LE RESEAU DE L'ADMINISTRATION.**

Tout usage d'un équipement personnel à des fins professionnelles se fait à mes risques et périls. Je ne pourrai prétendre à aucun dédommagement de la part de la Métropole en cas de dysfonctionnement de mon équipement ou de surcoût d'utilisation. Le Pôle Numérique n'assure aucun support ni aucune maintenance sur les équipements personnels.

Je peux être tenu pour responsable si un équipement personnel venait à perturber le bon fonctionnement du Système d'Information de la Métropole.

## 2.8. Usage sobre des outils numériques

### **J'AI CONSCIENCE DE L'IMPACT ENVIRONNEMENTAL DU NUMERIQUE ET ADOPTE UN COMPORTEMENT VERTUEUX.**

Je ne peux prétendre au renouvellement anticipé ou régulier d'un matériel numérique : le Pôle Numérique définit la stratégie de renouvellement des matériels et juge de leur éventuelle obsolescence.

Je prends soin et protège les matériels qui me sont confiés afin d'en prolonger la durée de vie.

Je respecte les procédures qui me sont communiquées par le Pôle Numérique pour réduire mon empreinte environnementale : notamment je ne démultiplie pas les destinataires en copie de mes mails, je ne crée pas des doublons des fichiers qui me sont transmis, je privilégie le partage de liens à l'envoi en copie de fichiers.

Je veille à l'extinction quotidienne des moyens numériques lorsque je termine mon activité quotidienne et met en veille mes équipements lorsque je ne les utilise pas notamment pour une pause.

#### **À RETENIR**

- **Je suis personnellement responsable des équipements mis à ma disposition.**
- **Comme mon code de carte bancaire, je ne communique mes identifiants de connexion à personne (mot de passe).**
- **Je suis responsable : je n'écris pas mon mot de passe sur un Post-It.**
- **Si mon smartphone personnel est contaminé à cause d'un usage professionnel, la Métropole ne peut en aucun cas être tenue responsable.**
- **J'adopte un comportement responsable qui vise un usage sobre et durable de mes outils numériques**

# 3. internet

## 3. INTERNET

### 3.1. Je me comporte comme un internaute responsable

Comme pour l'ensemble des moyens mis à ma disposition, Internet est destiné à un usage professionnel.

L'usage privé doit rester accessoire. Tout abus sera sanctionné. Je dois faire preuve, sur Internet comme dans l'exercice de mes fonctions, de professionnalisme, de discernement, de bon sens, de courtoisie et de prudence.

### 3.2. Téléchargements : attention !

Les téléchargements peuvent sérieusement perturber le fonctionnement du Système d'Information de la Métropole (accès ralentis pour les autres utilisateurs, impact possible sur l'utilisation d'applications métiers, conséquences sur les espaces disques, incompatibilité avec d'autres logiciels, introduction de virus, etc.).

Par ailleurs, les données circulant sur Internet peuvent être réglementées en termes d'utilisation ou être protégées par un droit de propriété intellectuelle.

**UN TELECHARGEMENT EST UN VECTEUR DE TRANSMISSIONS IMPORTANT DE VIRUS ; EN CAS D'INCIDENT, JE CONTACTE CATI.**

### 3.3. Filtrage Internet

L'accès Internet est un outil professionnel.

Dans ce cadre, la Métropole met en place un ensemble de mesures d'analyse et de filtrage des flux réseaux. Le filtrage vise à garantir la sécurité du système d'information de la Métropole :

- en évitant le téléchargement de données malveillantes,
- en filtrant l'accès à des sites dont la catégorisation est identifiée comme inappropriée,
- en contrôlant les fuites de données vers l'extérieur
- et en n'utilisant pas les réseaux métropolitains pour des besoins strictement privés ou récréatifs.

Pour cela, les outils mis en place concernent tous les agents avec l'attribution de droits par groupe : mes autorisations d'accès sont délivrées à la fois sur l'identification des sites accédés mais aussi sur la base d'une analyse automatisée des flux circulants.

- Le contrôle d'accès sur les sites visités se base sur la catégorisation du site, une liste blanche de sites spécifiquement autorisés et une liste noire de sites explicitement exclus. Un agent peut demander l'ouverture d'un site en liste blanche : l'administration statue au regard de l'adéquation de ce site avec les missions de l'agent et des contraintes de sécurité sur l'autorisation accordée. L'administration peut compléter les listes blanches ou noires au regard de ses propres enjeux opérationnels ou de sécurité.
- L'analyse automatisée des flux exclut l'inspection des données avec des sites catégorisés comme relevant du secteur bancaire ou du domaine de la santé.

Ce contrôle s'opère sur tout équipement professionnel métropolitain qu'il soit utilisé depuis le réseau interne de la Métropole ou depuis un réseau privé (domicile de l'agent en télétravail par exemple ou réseau public). Tout équipement personnel connecté aux réseaux métropolitains est filtré de la même manière.

L'analyse réalisée ne conserve pas mes données personnelles à l'exclusion des éléments cités ci-après (cf. §3.4).

La loi interdit l'accès à des sites de nature diffamatoire, discriminatoire, raciste, sexiste, révisionniste, pédophile ou incitant à la violence ou à la haine raciale ; en cas d'agissements de cette nature, ma responsabilité pénale personnelle peut être engagée, indépendamment des sanctions disciplinaires qui pourraient être prises.

**LE POLE NUMERIQUE CONTROLE ET LIMITE LES ACCES RESEAUX PAR CATEGORIE ET ANALYSE DE FLUX. JE PEUX DEMANDER LE DROIT D'ACCES A UN SITE BLOQUE EN CONTACTANT LE CENTRE D'ASSISTANCE TELECOM & INFORMATIQUE CATI ET EN JUSTIFIANT LE BESOIN PROFESSIONNEL.**

**SI J'AI BESOIN D'UN LOGICIEL OU D'UNE MISE A JOUR SPECIFIQUE, JE CONTACTE CATI.**

### 3.4. Qu'en est-il de ma navigation Internet ?

Lorsqu'un poste de travail accède à Internet, depuis un site de la métropole ou via un VPN, le serveur de connexion enregistre :

- L'identifiant de l'utilisateur,
- L'adresse du site web visité,
- Le nombre d'accès à ce site par l'utilisateur,
- Le nombre de sessions ouvertes par l'utilisateur,
- La durée totale de l'activité de l'utilisateur,
- Le volume des données transmises par l'utilisateur,
- L'adresse IP et le nom de l'équipement utilisé,
- Les motivations d'un éventuel blocage de flux,
- Les dates et heures des accès.

**Ces données sont conservées** sur support numérique pendant la durée maximale légale autorisée. Elles sont utilisées à des fins de statistiques, de dimensionnement des ressources, d'analyse ou de recherche de dysfonctionnement.

De plus, des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau conduisent à mettre en place un outil de mesure de la fréquence ou de la taille des fichiers de données téléchargés depuis le site Internet appelé.

Les éléments collectés par un tel outil permettent, à partir de la production de rapports quantitatifs et statistiques, d'intervenir sur la prévision de charge du réseau.

**TOUTEFOIS, CES INFORMATIONS COLLECTEES PEUVENT ETRE AMENEES A SERVIR, A POSTERIORI, DANS UN CONTEXTE D'ENQUETE POLICIERE.**

### 3.5. Usage de l'Intelligence Artificielle ?

L'intelligence artificielle (IA) est un processus visant à simuler certains traitements de l'intelligence humaine : elle repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique dynamique. Son but est de permettre à des ordinateurs d'imiter des raisonnements en se basant sur de l'apprentissage et en exploitant une grande quantité de données.

La Métropole s'engage à respecter un ensemble de principes éthiques dans l'usage de ces algorithmes aux premiers rangs desquels la Transparence, l'Équité, la Maîtrise Humaine, la Durabilité et la Sureté. Les outils numériques reposant sur de l'IA et développés par la Métropole, pour des besoins internes ou sur des services à la population respectent ces engagements.

Je m'engage à utiliser les outils mis à disposition de la Métropole en respectant ces principes éthiques.

D'autre part, je n'utilise pas des outils tiers (grand public ou non maîtrisés par la Métropole) basés sur de l'IA exfiltrant des données de la Métropole. En effet ces outils peuvent s'approprier ces données et les conditions de leur réutilisation ne sont pas connues ni garanties. Je ne peux notamment demander à ces moteurs d'IA d'analyser des données professionnelles ou de préparer des analyses en les contextualisant avec des éléments du domaine professionnel. Je pourrais être rendu responsable de la fuite de ces données.

#### À RETENIR

- **Un téléchargement est un vecteur de transmissions important de virus ; en cas d'incident : je contacte CATI.**
- **Ma navigation est filtrée par la Métropole ; Le Pôle Numérique conserve l'historique de mon activité de navigation sur Internet.**
- **Si j'ai besoin d'accéder à un site non autorisé, d'un logiciel ou d'une mise à jour spécifique, je contacte CATI.**
- **Je n'utilise pas des moteurs d'IA grand public avec des données professionnelles.**

# 4. outils collaboratifs



## 4. outils collaboratifs

### 4.1. La messagerie

#### 4.1.1. J'utilise la messagerie à des fins professionnelles

La messagerie est destinée à un usage professionnel. La diffusion large de messages à caractère privé n'est pas autorisée.

Je respecte les circuits de l'organisation ou la voie hiérarchique le cas échéant. Si je reçois un message par erreur, je le signale à l'expéditeur.

Je ne dois pas tenter de lire ou copier les courriels d'un autre utilisateur sans son autorisation expresse. Je m'abstiens également de toute tentative d'interception sans autorisation de courriels entre utilisateurs.

L'utilisation de la messagerie à des fins privées, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle n'affecte pas le trafic normal de la messagerie professionnelle.

Par défaut, tout courriel reçu ou envoyé à partir du poste de travail mis à ma disposition par la Métropole est considéré comme professionnel.

En cas d'absence prolongée, et pour les besoins du service, la Métropole peut accéder à ma messagerie. Cet accès peut être ouvert à mon responsable hiérarchique, après avis du délégué à la protection des données (DPO).

Seuls mes courriels privés identifiés comme tels sont protégés au titre du respect de ma vie privée et du secret de mes correspondances : la Métropole ne peut pas accéder à mes courriels privés, sauf dans le cadre d'une procédure d'enquête judiciaire ou sur autorisation d'un juge.

Pour que mes courriels privés soient protégés, je dois les identifier comme tels, par exemple :

- En précisant dans leur objet « Personnel » ou « Privé »,
- En les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

#### 4.1.2. J'évite les messages trop volumineux

Pour envoyer par Internet un fichier très volumineux ou de nombreuses pièces jointes, je peux utiliser un outil de compression pour ne faire qu'une pièce jointe compactée (fichiers ZIP). Pour l'échange de fichiers trop volumineux pour la messagerie, je contacte CATI pour obtenir la bonne procédure.

Pour un destinataire qui accède au même serveur de fichiers (en principe même direction), il peut être plus judicieux d'envoyer un lien ou un raccourci que le fichier lui-même.

#### 4.1.3. Concernant les courriels, je reste prudent et professionnel

Je peux être victime d'émetteurs indéliçables et recevoir, par exemple, un envoi massif de courrier non sollicité de nature commerciale, malveillant, raciste, propagandiste, etc. C'est ce qu'on appelle le « spamming ». En cas de doute, je m'adresse au Centre d'Assistance Télécom & Informatique CATI. De manière générale, j'évite de m'inscrire à des listes de diffusion dont je ne suis pas totalement sûr.

Attention à l'hameçonnage : je veille à ne pas ouvrir les courriels dont l'objet paraîtrait suspect. Je ne clique pas non plus sur les liens si j'ai un doute.

Enfin, pour éviter l'intrusion et surtout la propagation des virus, je n'ouvre jamais des pièces jointes suspectes (émetteur inconnu), fichiers avec un suffixe en .exe.

Il est préférable de supprimer le message puis de vider le dossier « éléments supprimés ».

**LE POLE NUMERIQUE PEUT BLOQUER PONCTUELLEMENT UN TYPE DE FICHIER JOINT EN CAS DE NECESSITE OU SUPPRIMER D'AUTORITE DES MESSAGES IDENTIFIES DANGEREUX DANS L'ENSEMBLE DES BOITES MAILS DE LA METROPOLE.**

**JE SIGNALE TOUT COURRIEL MALVEILLANT AU POLE NUMERIQUE AVEC LE BOUTON D'ALERTE PHISHING.**



#### 4.2. Partage de documents

Si je dois partager des documents avec des destinataires en interne, mais aussi avec l'extérieur, je contacte CATI pour connaître les solutions validées par la Métropole.

J'applique les précautions suivantes pour éviter que des données confidentielles de la Métropole se retrouvent exposées à l'extérieur de l'organisation :

- Bien organiser mes données permettra d'avoir une vision claire des documents et des partages qui leurs sont associés.
- Être vigilant sur les éléments partagés en fonction de leur degré de confidentialité.
- Assurer le bon suivi de la gestion des droits d'accès que j'ai donnés, et exiger l'authentification des personnes à qui j'ai donné les droits d'accès.
- Être vigilant sur les fichiers tiers qui sont partagés avec moi.

#### 4.3. Propriété des données

Les données que je produis dans un cadre professionnel sont la propriété de la métropole, quel que soit leur format :

- message électronique,
- fichier bureautique,
- photographie,
- film,
- dessin,
- coordonnée géographique,
- etc.

Ces données doivent être partagées avec les autres agents habilités et susceptibles de travailler sur les mêmes dossiers. C'est pourquoi, sauf si c'est techniquement impossible, j'enregistre les documents et les données que je produis sur les serveurs de la métropole ou sur les applicatifs métiers (type office 365), en veillant :

- à enregistrer ces données dans un répertoire adapté, pour limiter leur accès aux personnes habilitées,
- à ne pas copier ces données plusieurs fois, pour éviter d'accroître l'espace de stockage.

#### À RETENIR

- **J'utilise la messagerie à des fins professionnelles.**
- **Je cible mes destinataires.**
- **J'évite les messages trop volumineux.**
- **Concernant les courriels, je reste prudent et professionnel.**
- **Je signale tout courrier malveillant au Pôle Numérique avec le bouton d'ALERTE PHISHING.**
- **Les données que je produis appartiennent à la Métropole.**

## 5. BUREAUTIQUE



## 5. bureautique

### 5.1. La sécurité, ça me concerne aussi

D'une manière générale, la sécurité informatique consiste à s'assurer que les ressources matérielles et logicielles de l'entreprise sont uniquement utilisées dans le cadre prévu à cet effet afin de limiter les risques. La sécurité informatique vise donc à garantir **l'intégrité, la confidentialité** des données ainsi que la **disponibilité** du Système d'Information.

**L'homogénéité des postes de travail** est une condition indispensable pour maîtriser l'intégration des composants, leur déploiement et leur administration :

- Je ne modifie pas la configuration de mon poste de travail sans l'intervention du Pôle Numérique : pas d'installation de logiciels, pas d'ajout de matériels. Pour toute demande d'installation de logiciel sur mon poste de travail, qu'il soit gratuit ou payant, je contacte CATI.
- Chaque poste de travail correspond à une configuration type, adaptée à mon profil professionnel (applications auxquelles j'ai accès). Si une réinstallation est nécessaire, elle sera faite sur les bases de cette configuration répertoriée.
- Je suis également responsable de l'utilisation que je fais des ressources informatiques ; je ne dois pas effectuer d'opérations pouvant nuire au bon fonctionnement des systèmes et à leur intégrité (intervention sur des fichiers systèmes, par exemple).

Ma clé d'entrée : le code d'accès au Système d'Information

Il est composé du nom de l'utilisateur (LOGIN) et de son mot de passe. Il permet de gérer la confidentialité des données auxquelles j'ai accès.

Le code d'accès et le mot de passe sont personnels, je ne dois en aucun cas le communiquer à un autre utilisateur qui pourrait alors l'utiliser dans l'intention de nuire à l'intégrité des données dont j'ai la responsabilité.

Pour consolider cette confidentialité, je change le mot de passe régulièrement (les modalités sont décrites sur M ACTU).

Je m'engage expressément à :

- ne pas masquer ma véritable identité ;
- ne pas usurper l'identité d'autrui ;
- ne pas quitter mon poste de travail en laissant mon poste accessible ;
- ne jamais « prêter » mon compte ;
- signaler à CATI toute violation ou toute tentative de violation suspectée de mon compte informatique et, de façon générale, toute anomalie constatée (problèmes d'initialisation, mauvais fonctionnement, ...).
- ne pas introduire « de ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du Système d'Information,
- éteindre mon poste de travail en fin d'activité.

**SI J'AI BESOIN D'ACCÉDER À UNE NOUVELLE APPLICATION, JE FAIS LA DEMANDE À CATI.**

### 5.2. Que dois-je faire pour éviter les virus ?

Les virus représentent l'une des menaces capables de mettre en cause la sécurité et l'intégrité du réseau de la Métropole. Les serveurs et les postes de travail sont équipés d'antivirus.

Pour éviter les risques, il convient de veiller à la fiabilité des fichiers provenant de sources extérieures et qui se connectent au réseau de la Métropole. Je fais particulièrement attention aux clés USB dont je ne connais pas la provenance.

Le Pôle Numérique met en place un ensemble d'outils de sécurisation.

Il est strictement interdit de désactiver les systèmes de protection du poste de travail.

En cas de doute concernant l'origine, la taille, le type de fichier ou l'objet d'un message, je relève un maximum d'éléments caractéristiques qui permettront d'analyser la cause exacte de l'incident (ex : copie d'écran du message d'erreur, mail infesté, message d'erreur donné, etc., ...).

Je n'utilise pas ce fichier ou message et je contacte le Centre d'Assistance Télécom & Informatique (CATI).

### 5.3. Mon utilisation peut être tracée

Le Pôle Numérique est responsable du bon fonctionnement des moyens informatiques et de communication. La Métropole est responsable juridiquement des accès effectués par les utilisateurs sur son Système d'Information ; ceux-ci sont conservés en respectant les durées légales.

Elle doit assurer une disponibilité maximale des différents moyens qu'elle met à la disposition des utilisateurs, dans le respect des budgets alloués et de la réglementation (propriété intellectuelle).

Le Pôle Numérique est chargé de veiller au respect des règles d'usages énoncées dans la présente charte. Les techniciens du Pôle Numérique peuvent être amenés, dans le cadre de leurs fonctions, à accéder à des informations à des fins de diagnostic ou d'administration ; ils ont l'obligation de préserver la confidentialité des informations auxquelles ils accèdent lors d'interventions.

Le Pôle Numérique utilise des outils destinés à contrôler l'usage qui est fait de mon poste de travail (installation de logiciels, ajout de matériels, navigation internet, etc., ...)

En fonction des manquements constatés et au regard des risques évalués par le Pôle Numérique, ce dernier se réserve le droit de :

- modifier ou suspendre mes droits d'accès au Système d'Information,
- informer mon responsable hiérarchique.

Si des anomalies sont détectées ou suspectées, des mesures de contrôle individuel par poste de travail pourront être mises en place après information.

### 5.4. Utilisation des fichiers

Je ne dois pas tenter de lire ou copier les fichiers d'un autre utilisateur sans son autorisation expresse.

Par défaut, les fichiers présents sur les serveurs, dans le cloud ou sur mon poste de travail ont un caractère professionnel et l'administration peut les consulter librement, y compris en dehors de ma présence.

Seuls mes fichiers privés sont protégés au titre du respect de ma vie privée ; la Métropole ne peut accéder à mes fichiers privés identifiés comme tels qu'en ma présence, après m'avoir appelé, ou en cas de risque ou d'événement particulier.

Pour que ces fichiers privés soient protégés, je dois les identifier comme tels, par exemple :

- en précisant dans leur nom « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé »

**J'ÉVITE DE STOCKER DES FICHIERS SUR MON POSTE DE TRAVAIL ET JE PRIVILEGIE AUTANT QUE POSSIBLE LE STOCKAGE ET L'ENREGISTREMENT SUR LE SERVEUR DE LA METROPOLE.**

### 5.5. Perte ou vol de matériel informatique

En cas de vol ou de perte je dois, le plus rapidement possible :

- me rendre au commissariat le plus proche pour faire une déclaration de vol.
- déclarer l'incident à CATI et y joindre la déclaration de vol.

Je dois signaler au Centre d'Assistance Télécom & Informatique CATI tous les cas de dysfonctionnements, de casse, de perte, de vol, de difficultés d'utilisation, de changement de situation.

#### À RETENIR

- Lorsque je m'absente momentanément, je verrouille préalablement ma session Windows.
- Je ne mets pas les fichiers communs ou partagés sur mon espace personnel ou sur mon poste de travail.
- J'éteins mon poste de travail lorsque je quitte mon lieu de travail.
- Lorsque je crée des documents, pour des raisons de facilité de partage et de sécurité (sauvegarde), je les enregistre sur le serveur de fichier.
- Je n'utilise pas mon poste de travail pour stocker des données car en cas de changement de matériel, elles ne seront pas récupérées.

## 6. TÉLÉPHONIE



## 6. téléphonie

### 6.1. Je maîtrise mon temps de communication

L'usage des téléphones est réservé aux besoins professionnels. Un usage ponctuel du téléphone pour des communications personnelles est toléré à condition que cela n'entrave pas l'activité professionnelle.

Je respecte les usages et **je maîtrise mes dépenses.**

### 6.2. Si je suis doté d'un téléphone mobile professionnel

**Je connais les limites.** Si j'ai un doute, je demande au Centre d'Assistance Télécom & Informatique CATI les caractéristiques de mon forfait (durée, options, ...) et je veille à respecter le cadre prévu par le forfait.

Les appels vers les numéros de services commençant par 08 (hors numéros gratuits), les appels de ou vers l'étranger, et les téléchargements de sonneries et autres logos sont tous facturés hors forfait et seront à ma charge.

En cas de vol ou de perte je dois, le plus rapidement possible :

- appeler le service client de l'opérateur pour bloquer la ligne (information disponible sur le document signé, fourni lors de la remise de l'équipement).
- me rendre au commissariat le plus proche pour faire une déclaration de vol.
- déclarer l'incident à CATI et y joindre la déclaration de vol.

Je dois signaler au Centre d'Assistance Télécom & Informatique CATI tous les cas de dysfonctionnements, de casse, de perte, de vol, de difficultés d'utilisation, de changement de situation.

L'utilisation de mon portable est liée à mon emploi, par conséquent, tout changement de fonction peut entraîner la reprise de l'équipement.

### 6.3. Qu'en est-il de ma consommation téléphonique ?

Pour chaque ligne téléphonique, une facture détaillée anonymisée des numéros composés par l'utilisateur peut être éditée et transmise à son responsable hiérarchique.

Poste par poste, les dates et heures des appels sortants avec les durées, les coûts et numéros appelés sont stockés et conservés pendant la durée maximale légale afin de permettre le contrôle des factures, le suivi statistique et la réalisation d'études en vue de la réduction des coûts ou d'un meilleur dimensionnement du service. Ce suivi est effectué tant pour le téléphone fixe que pour les mobiles.

Les comportements abusifs sont signalés ; de plus, les comportements abusifs répétitifs pourront faire l'objet de restriction de ligne ou de sanction.

#### À RETENIR

- **Je protège l'utilisation de mon téléphone portable avec un code secret.**
- **En cas de vol ou de perte j'appelle le service client de l'opérateur pour bloquer la ligne, je déclare le vol au commissariat le plus proche et j'informe CATI.**
- **Ma consommation téléphonique est suivie.**
- **Je maîtrise ma consommation data en privilégiant la connexion WiFi.**



## 7. je quitte la métropolole

## 7. je quitte la métropole

J'anticipe mon départ en prévenant mes interlocuteurs et informe CATI que je quitte l'institution. Avant mon départ, j'organise la restitution des équipements mis à ma disposition.

### 7.1. Messagerie

Lorsque je quitte définitivement la Métropole, sauf exception, mon compte de messagerie sera supprimé dans un délai maximum de 3 mois.

Je veille à nettoyer ma messagerie de mes messages privés ou personnels : après mon départ, la métropole peut accéder à tous les messages professionnels

### 7.2. Bureautique

J'anticipe mon départ en sauvegardant l'ensemble des fichiers sur l'espace partagé de ma direction pour assurer la continuité de service. Tous les documents et toutes les données créés sont la propriété de la Métropole. Je ne peux en aucun cas les copier ni les emporter avec moi en-dehors de l'institution.

Je me rapproche de CATI pour accomplir les modalités de restitution de mes équipements. Mon poste informatique pourra être réutilisé après mon départ et sans mon consentement.

### 7.3. Téléphonie

Je prends contact avec le Centre d'Assistance Télécom & Informatique CATI pour faire suspendre ma ligne mobile et accomplir les modalités de restitution de mes équipements mobiles (téléphone mobile, tablette et les accessoires).

Je prends la précaution de supprimer toute information personnelle de mes équipements mobiles car il sera réutilisé.

#### À RETENIR

Avant mon départ :

- Je ne conserve pas de copie des fichiers professionnels,
- Je supprime les courriels privés de ma boîte de messagerie,
- Je supprime les contenus personnels de mon poste informatique,
- Je supprime mes données personnelles de mon téléphone mobile,
- J'organise la restitution des équipements mis à ma disposition.

## 8. contacts

Pour toute question relative au système d'information, aux applications métiers et aux moyens de communication :



**99999** (en interne)  
**04 88 77 62 37** (depuis le réseau opérateur)  
**cati@ampmetropole.fr**  
**cati.ampmetropole.fr** (à privilégier)

Pour la prévention des situations de harcèlement ou de discrimination :

Par courrier uniquement, sous double enveloppe cachetée, avec la mention « CONFIDENTIEL » à l'adresse suivante :

**Commission de recueil des signalements de la Métropole Aix-Marseille-Provence**  
**Tour La Marseillaise**  
**2 quai d'Arc - 13002 MARSEILLE**

Pour toute question relative à la protection des données à caractère personnel :

**dpo@ampmetropole.fr**

