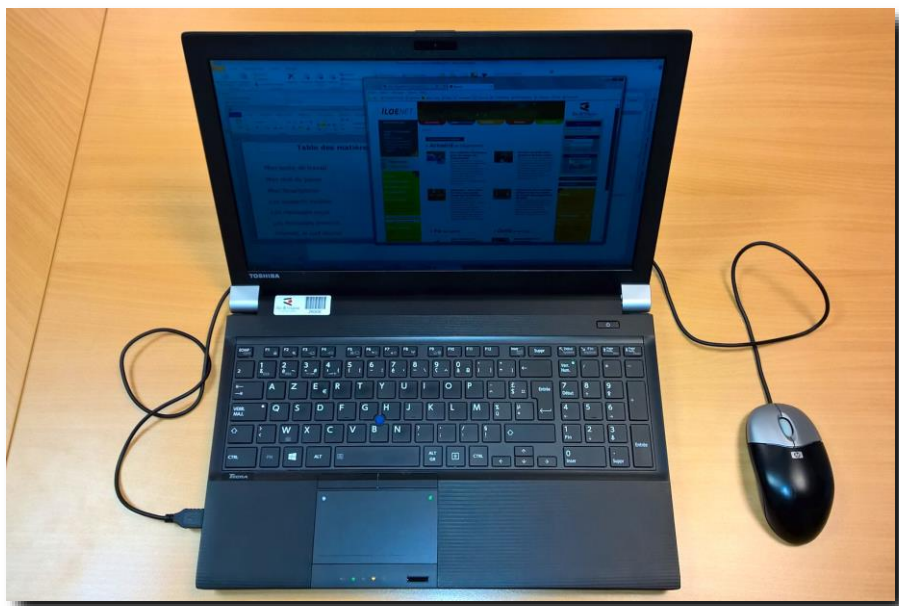


La sécurité de nos informations

Petit manuel de bonnes pratiques



À consommer sans modération

Table des matières

Introduction	3
Soyons discrets.....	3
La messagerie	4
Mes mots de passe.....	7
Mon matériel	8
Les réseaux sociaux	11
Internet	12
Mes données	13
Mon bureau et mes dossiers papier	14
Qui peut voir ce que je fais ?	15
Numéros utiles.....	15

Introduction

Pourquoi ce manuel ?

La charte d'usage du système d'information est un document obligatoire et important : elle constitue la référence en matière de droits et de devoirs de l'utilisateur.

Toutefois la mise en application des règles de la charte peut paraître difficile et fastidieuse, aussi vous est-il proposé ce « petit manuel de bonnes pratiques » qui est un document d'accompagnement qui vous permet d'acquérir les bons réflexes.

La valeur d'une information dépend de la personne qui la consulte : ce qui est important pour moi ne l'est pas pour d'autres et inversement. Ainsi le premier brouillon d'un futur marché public peut intéresser pas mal monde ! Mais que dire si un tiers prenait connaissance du dossier d'accompagnement d'une famille par notre collectivité ?

Ce livret vous propose aimablement quelques gestes simples et pratiques, ayant le bon goût d'être *aussi utiles dans le cadre du travail qu'à la maison*.

N'hésitez pas à vous rapprocher de votre correspondant bureautique...

Soyons discrets

Au bureau, dans l'espace public, à la maison ou sur les réseaux sociaux, gardez à l'esprit que vous manipulez des informations qui ont une valeur pour le département ou pour la vie privée des usagers.

Faites preuve de la plus grande discrétion dans vos échanges.
Petit manuel de bonnes pratiques — Document interne - page 3

Les cyberattaques ont souvent pour point de départ des actions d'ingénierie sociale.

L'ingénierie sociale est une manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes (*Source : ANSSI*).

Les techniques d'ingénierie sociale les plus connues sont l'envoi de courriers électronique piégés (pour les rançongiciels notamment) ou de faux courriers électroniques demandant un paiement en urgence (« fraude au président »).

Si les attaques non ciblées de ce type sont facilement identifiables (incohérences, fautes de français, etc.), les attaquants peuvent analyser l'environnement du département en récupérant des informations publiées sur internet (organigramme, profils LinkedIn, messages sur les réseaux sociaux, etc.) et lancer des attaques ciblées beaucoup plus complexes à déjouer.

La messagerie

Les messages reçus

Un petit clic sur le lien dans le message, juste pour voir : je ne risque rien !

La plupart des canulars, escroqueries, introduction de logiciels-espions, de virus... commencent par la réception d'un mail à l'air innocent, menaçant, utile ou amusant. Dans tous les cas, un lien à cliquer ou une pièce jointe à ouvrir contiennent la menace.

Quelques bonnes pratiques

Un message peut provenir d'un autre expéditeur que celui indiqué aussi je considère tout lien dans un message reçu comme suspect, même si je pense bien connaître l'expéditeur.

Je n'ouvre aucune pièce jointe que je n'attends pas surtout si elle est associée à un message « pressant » ou « menaçant ».

Si le lien semble sérieux et intéressant, je le recopie dans mon navigateur et vais sur le site de cette façon.

Au moindre doute, je crée un incident sur @telier.

Lorsque je rédige un message, je m'assure des destinataires avant d'envoyer le message. Soyez vigilant avec l'usage des listes de diffusion qui peuvent contenir des personnes qui n'ont pas à connaître les informations.

Le saviez-vous ?

Le truc : la plupart des liens et images dans les messages publicitaires permettent à l'expéditeur de savoir que vous lisez bien son courrier. Plus vous cliquez, plus vous en recevrez.

L'autre truc : passer la souris sur le lien sans cliquer. L'adresse internet vraie apparaît et si elle n'a rien à voir avec le lien, il s'agit sûrement d'un piège.

En cliquant sur le « + » d'un groupe de diffusion, vous pouvez connaître le détail des destinataires du groupe.

Les messages envoyés

OUPS ! J'ai cliqué sur « répondre à tous » au lieu « répondre » en choisissant une personne...

Une fois un message envoyé, rien ne permet de le récupérer.
Si le message est envoyé à des destinataires non prévus, c'est trop tard.

De plus le message que j'envoie est un peu l'ambassadeur du département : ce que j'y écris véhicule l'image de marque du département !

Quelques bonnes pratiques

Je prends mon temps pour faire partir un message, je vérifie les destinataires et je suis prudent avec les destinataires par défaut proposés par la messagerie.

Je reste toujours courtois, je ne tiens jamais de propos contraires à la loi (injures, xénophobie, racisme, etc.), même sous une forme humoristique, qui pourrait me nuire ou nuire à l'image du département.

Je considère que les messages peuvent être lus ou transférés à mon insu : je n'y mets aucune information que je considère comme sensible (personnelle ou professionnelle).

Pour des échanges de données avec des partenaires, le département peut nous proposer des outils sécurisés.

La transmission de chaîne de lettres (canulars, appels à la générosité, etc.) est interdite.

Le saviez-vous ?

Faites une pause avant de valider un message écrit sous le coup de l'émotion (ex. : colère). Relisez-le ensuite au calme.

Mes mots de passe

Suis-je vraiment le seul à connaître mon mot de passe ?

Il est l'ultime protection pour l'accès aux ressources auxquelles j'ai droit. Couplé à mon nom d'utilisateur, il fait partie de mon identité numérique et il est, à ce titre, placé sous ma seule responsabilité.

Je suis entièrement responsable des actions réalisées grâce à mon mot de passe, même s'il est avéré que quelqu'un d'autre l'a utilisé.

Quelques bonnes pratiques

Je le choisis robuste et facile à retenir en utilisant par exemple :

- La méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » -> 1tvmQ2tl'A
- La méthode phonétique : « J'ai acheté huit CD pour cent euros cet après-midi » -> ght8CD%E7am

Source : Cybermalveillance.gouv.fr

Utilisez un gestionnaire de mots de passe (ex : KeePass) afin de stocker vos différents mots de passe.

Personne d'autre que moi ne connaît mon mot de passe. Je ne le communique sous aucun prétexte.

De même, je ne demande à personne de me donner le sien, ni aimablement ni en usant de mon autorité hiérarchique.

En cas d'absence ou de nécessité de service, il existe des systèmes de délégation pour la messagerie et l'agenda. Je me renseigne avant de partir. De même, les documents stockés sur le réseau peuvent également être facilement partagés.

Le saviez-vous ?

En essayant « 123456 », « password » et « 12345678 » vous accédez à 10 % des comptes sur internet, tandis que « 1234 » déverrouille 10 % des cartes SIM.

Il existe des sites Internet qui proposent de tester vos mots de passe. Privilégiez le site de l'[ANSSI](#) qui vous permet de calculer la « force » d'un mot de passe sans le diffuser à un tiers inconnu...

Mon matériel

Mon ordinateur professionnel

Suis-je bien le seul à l'utiliser ?

L'actualité nous le montre : mon PC est convoité, il est agressé par des virus, certains essaient d'en dérober le contenu... discrètement.

C'est mon outil, il a de la valeur pour moi... et pour d'autres ! Ce qu'il contient est précieux aussi : ayons au moins quelques gestes simples pour éviter la plupart des ennuis.

Quelques bonnes pratiques

Je l'éteins le soir : En se rallumant, l'antivirus sera à jour.

Si c'est un portable, je le garde sous ma surveillance dans les lieux publics et je l'attache à mon bureau : quelques secondes suffisent à le dérober !

Je sauvegarde mes données sur les outils mis à disposition par la DSN : la ruche SharePoint pour les documents sensibles et Microsoft Teams pour les documents non-sensibles. Mon disque dur n'est pas

éternel et ne prévient pas avant un souci de fiabilité donc je n'y conserve aucun document important.

Je le verrouille en quittant le bureau : si quelqu'un l'utilise, il peut tout faire... en se faisant passer pour moi !

Si son comportement devient bizarre (lenteurs aléatoires, affichage d'écrans non voulus...), peut-être a-t-il un virus : je débranche toutes les prises, y compris l'alimentation et je contacte le support informatique.

Le saviez-vous ?

La combinaison  +  verrouille votre PC !

Mon Smartphone professionnel

Le smartphone est avant tout un ordinateur, avec lequel je peux, parfois, téléphoner.

L'ennui c'est qu'il a tendance à donner aux fournisseurs d'applications toutes mes données personnelles et professionnelles, ainsi que ma localisation, discrètement et sans me demander mon avis...

Quelques bonnes pratiques

J'active le verrouillage (choisir un code ou un schéma). En cas de perte ou de vol, mes données seront davantage protégées.

Je préviens immédiatement le support si mon compte professionnel est paramétré sur un téléphone perdu.

Je n'installe aucune application en dehors des « stores » officiels (Play Store pour Android) et je vérifie les autorisations que je donne aux applications installées : certaines pillent nos contacts, agendas,

messages, envoient des SMS surtaxés sans aucun scrupule, en échange d'un service minime ! Protégeons nos informations ainsi que celles de nos amis et de nos collègues !

Je le mets à jour régulièrement.

Je ne prête pas mon smartphone à un inconnu et je refuse systématiquement que l'on m'installe une application (même pour gagner 1 % sur ses courses ou participer à un concours).

Le saviez-vous ?

L'application du plus grand site de commerce en ligne vous géolocalise tant qu'elle est installée.

Le Département utilise un outil de supervision des smartphones. Il permet de garantir la sécurité du smartphone, en repérant toute anomalie sur ce dernier. Il est possible que des mises à jour s'effectuent à distance la nuit ou le weekend.

Mon matériel personnel

Je ne connecte aucun matériel personnel ou inconnu (prêté, trouvé...) au réseau interne du département. Les équipements personnels ou de visiteurs peuvent utiliser le Wi-Fi « invité ».

Je suis seul responsable de l'usage d'outils personnels, en particulier des applications sur le smartphone que j'ai installées.

Les réseaux sociaux

Les réseaux sociaux

Au départ conçus comme des chaînes d'amitié, ils sont vite devenus des mines d'information — les miennes ! – pour toutes sortes d'usages.

Tout ce que j'y mets est lu, analysé et exploité, il n'y a aucun contrôle d'identité sur les gens qui m'approchent, tous les détails que je fournis sur moi sont stockés, souvent à l'étranger où la loi européenne ne s'applique pas.

Il y a toujours une aimable pression pour que je « dise vrai » et que je « complète mon profil ». Pourquoi au juste ?

Quelques bonnes pratiques

Je me pose la question de l'utilité d'y parler de moi : qui lira ? Qui exploitera ? Je ne sais pas.

Je vérifie dans la vraie vie que « l'ami » qui veut m'approcher est bien celui qu'il prétend être.

Je ne mets aucune donnée professionnelle ou d'identification : service, mission, adresse, téléphone, dates de vacances... et je montre l'exemple à mes proches et enfants.

Je ne participe aux réseaux sociaux à des fins professionnelles qu'avec l'aval de ma hiérarchie.

Le saviez-vous ?

Les cambrioleurs exploitent les réseaux sociaux depuis des années pour visiter vos maisons durant vos déplacements.

Internet

Internet (ou le mythe du surf discret)

La navigation sur Internet est tout sauf anonyme et discrète. Toute mon activité : mes recherches, les sites que je visite... est tracée, enregistrée et utilisée.

Certains sites proposent des logiciels malveillants sous la forme d'outils miracles, barres d'outils, économiseurs d'écran... c'est pour cela que le filtrage du département ne m'autorise pas tous les sites.

Enfin, l'information que j'y trouve n'est pas forcément fiable...

Quelques bonnes pratiques

Comme dans la vraie vie, j'évite les sites peu fréquentables.

Je ne prends pas tous les écrits pour argent comptant.

Je n'utilise pas mon adresse mail professionnelle pour un service internet « personnel » (les impôts, par exemple) car j'aurais beaucoup de mal à l'utiliser en cas de départ.

À la maison, mon antivirus est à jour et je peux me renseigner sur des outils et paramètres pour rendre ma navigation moins « analysable ». Certains navigateurs ou outils de recherche sont plus respectueux de votre vie privée.

Le saviez-vous ?

La loi exige que le département (comme tout fournisseur d'accès) conserve les traces de vos connexions sur internet pendant une année.

Mes données

Mes documents professionnels sont-ils bien protégés ?

Les documents stockés en local sur mon ordinateur ne sont pas sauvegardés. Les disques durs d'ordinateur et a fortiori les supports amovibles rendent les documents très vulnérables à la perte ou à la diffusion accidentelle.

Les supports amovibles sont interdits et les données professionnelles nécessitant une sauvegarde doivent être enregistrés sur les outils mis à disposition par la DSN.

Quelques bonnes pratiques

Je stocke mes documents professionnels dans les espaces mis à disposition par la DSN qui sont aptes à gérer la conservation et la confidentialité.

Je ne cumule pas les fichiers inutilement, je supprime régulièrement les données obsolètes. Garder des archives de messagerie sur plusieurs années ou des documents de travail relatifs à des projets achevés ou abandonnés augmente inutilement les besoins de stockage et rend la recherche d'informations réellement utiles plus difficile.

Je suis responsable de la fin de vie des données que je manipule. Je m'assure de respecter les durées de conservation des données personnelles (telles que déclarées dans le registre des traitements).

Le saviez-vous ?

Le service de préarchivage est là pour vous aider pour toute question préalable à l'archivage ou la purge.

Toute perte de fichier contenant des données à caractère personnel constitue une violation de données et doit être déclarée à la CNIL dans les 72 heures. Contactez systématiquement votre DPO.

Mon bureau et mes dossiers papier

Mon bureau, mon lieu de travail

Les visiteurs indéliçats ne sont pas toujours faciles à repérer, surtout à l'heure de midi...

Mes écrits peuvent être très sensibles (données sur les familles, futurs tracés de routes) ou simplement intéresser les sociétés qui souhaitent connaître et remporter les marchés publics... et savoir comment je travaille avec leurs concurrents.

Certains visiteurs, aimables, mais peu scrupuleux, abusent parfois de la confiance qui règne dans notre lieu de travail : coup d'œil dans les bureaux vides à l'heure de midi, passage à l'imprimante dans le couloir...

Quelques bonnes pratiques

En quittant mon bureau, je range les dossiers, cartes de visite... j'efface le tableau blanc, je ferme la porte.

Je détruis les feuilles du tableau de papier en réunion après usage, j'efface le tableau blanc.

Je récupère rapidement mes documents sur l'imprimante et je m'assure qu'aucun document sensible n'y demeure.

J'accompagne aimablement mon visiteur pendant toute sa visite de l'entrée jusqu'à la sortie, même s'il me connaît, même s'il connaît le chemin, même si j'ai hâte d'aller déjeuner...

Pensez à récupérer vos documents dès qu'ils sont imprimés.

Un document traîne à l'imprimante, pensez à le rendre à son propriétaire.

Le saviez-vous ?

Certains commerciaux ont pour règle de prendre rendez-vous en fin de matinée afin de profiter d'une circulation aisée le midi dans des bureaux déserts... C'est leur mission de collecter toute information qui peut apporter du travail à leur entreprise.

Qui peut voir ce que je fais ?

D'une manière générale, mon activité et ma vie privée sont protégées.

Cependant, je dois savoir que :

- Les administrateurs système peuvent accéder à l'ensemble des espaces mémoire des ordinateurs du département ;
- Les courriers électroniques peuvent également être visibles par les administrateurs système ;
- Toutes mes connexions internet réalisées depuis le département sont tracées. La durée légale de conservation de ces traces est d'un an.

Mes espaces mémoire et courriers électroniques marqués « PERSONNEL », « PERSO », « PRIVE » ne sont consultables par un administrateur que dans le cadre du traitement d'un incident et dans le respect des règles de la charte administrateur.

Numéros utiles

En cas de problème, demande ou question, vous pouvez contacter différentes instances.

Si vous rencontrez un souci lors de l'utilisation d'une application métier, si vos collègues directs ne sont d'aucun secours, vous pouvez contacter le RSIM en charge de l'application ou le centre de service de la DSN. Le centre de service connaît tous les RSIM.

Si vous rencontrez un souci avec des équipements informatiques, vous pouvez contacter votre correspondant bureautique ou le centre de service de la DSN.

Pour toute demande de moyen (droits d'accès, matériel, etc.), vous devez contacter les correspondants informatiques. Les demandes sont généralement soumises à une validation hiérarchique.

Pour tout souci de sécurité, vous pouvez contacter votre correspondant informatique ou le centre de service de la DSN. Ne laissez pas un problème de sécurité en suspens !

Pour toute question (non urgente) relative à la sécurité de l'information, vous pouvez contacter le chargé de mission gestion des risques numériques de la DSN.

Pour toute question relative à la gestion des données concernant les gens (agents, usagers, etc.), vous devez contacter le DPO de la collectivité.

Le chargé de mission gestion des risques numériques de la DSN	Téléphone : 0299022131 Messagerie : clement.le-corre@ille-et-vilaine.fr
Le DPO	Téléphone : 0299023305 Messagerie : dpo@ille-et-vilaine.fr

En cas d'urgence, le centre de service	Téléphone : 40.40 Messagerie : 4040@ille-et-vilaine.fr
--	---



Charte d'utilisation du système d'information Version 2021.12

1	Introduction	3
1.1	Objet.....	3
1.2	Lexique	3
1.3	Portée.....	4
1.4	Diffusion	4
2	Usage des ressources et règles d'utilisation	5
2.1	Usage professionnel des ressources	5
2.2	Usage personnel des ressources	5
2.3	Arrivées, changements de postes et départs.....	5
2.3.1	Affectations et bon usage des ressources.....	5
2.3.2	Départ.....	6
2.3.3	La nécessité de continuité de service	7
2.4	Télétravail et mobilités	7
2.5	Internet, la messagerie et les réseaux sociaux.....	8
2.5.1	La messagerie	8
2.6	Utilisation de ressources tierces	9
2.7	Droit à la déconnexion	10
2.8	Responsabilité des utilisateurs.....	10
3	Protection de la vie privée	12
3.1	Traitement des données personnelles	12
3.2	Confidentialité des données personnelles.....	13
3.3	Contrôles automatisés	13
4	Mesures de contrôle de l'utilisation des ressources	15
5	Charte administrateur	16
5.1	Principes généraux à respecter	16
5.1.1	Principe de finalité et de maîtrise des droits	16
5.1.2	Principe de confidentialité	17
5.1.3	Principe de moindre gêne et d'information des utilisateurs.....	17
5.2	La surveillance et le contrôle	18
5.3	Le traitement des dysfonctionnements et incidents de sécurité.....	19
5.3.1	Contrôle et manipulation des données personnelles dans le cadre d'un incident	19
5.3.2	La préservation des preuves	21
6	Sanctions	22
7	Textes de référence.....	23

1 Introduction

1.1 Objet

La présente charte a pour objectif de protéger le patrimoine et l'image du département en faisant de l'utilisateur un acteur essentiel de la démarche de sécurisation du système d'information.

Elle définit les droits et devoirs de chaque utilisateur du système d'information mis à disposition par le département.

Afin d'aider les utilisateurs à adopter les bons réflexes d'utilisation du système d'information, un « Petit manuel de bonnes pratiques » reprend les éléments de la charte sous la forme de « cas d'usages ».

1.2 Lexique

Système d'information : ensemble des ressources permettant de collecter, stocker, traiter et distribuer de l'information. Ces ressources sont mises en œuvre par le département pour ses besoins propres ou ceux de ses partenaires ou des usagers.

Le système d'information du département est composé :

- Des équipements informatiques et téléphoniques, incluant notamment : postes de travail fixes et portables, serveurs, actifs réseau, imprimantes, scanners, téléphones fixes et mobiles, fax, tablettes ;
- Des outils, applications et logiciels permettant la création, la modification, l'échange, la diffusion, la reproduction, le stockage et la suppression des informations ;
- Des données et informations (fichiers bureautiques, code source, écrits, images, sons et vidéos).

Utilisateur : Toute personne utilisant le système d'information du Département.

Administrateur (ou administrateur informatique) : Toute personne, quel que soit son statut, ayant en charge sur le système d'information du département :

- Des actions d'administration ou d'exploitation – incluant l'installation, la configuration, la maintenance, le support et l'évolution ;
- Et des actions de sécurisation et de contrôle des ressources physiques et logiques.

Données à caractère personnel : Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique peut être identifiée directement (exemple : nom et prénom) ou indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image). *Source : cnil.fr*

Délégué à la protection des données (DPO) : Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. *Source : cnil.fr*

Violation de données : Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles. *Source : cnil.fr*

Moyens d'authentification : couple identifiant / mot de passe permettant de s'authentifier pour l'ouverture de son ordinateur ou dans une application informatique comme la messagerie, ou une application métier, etc.

1.3 Portée

L'ensemble du système d'information du département est soumis aux règles définies dans la présente charte.

Ces règles s'imposent à tout utilisateur du système d'information du département, et ce quel que soit son statut (agents de la fonction publique, salariés de droit privé, stagiaires, personnes en contrat d'apprentissage, intervenants extérieurs, élus, etc.).

1.4 Diffusion

La présente charte est annexée au règlement du temps de travail, elle s'impose à l'ensemble des agents du département, et en suit les règles d'entrée en vigueur.

La présente charte est portée à la connaissance des agents du département
Elle s'applique également aux personnes qui utilisent ou accèdent temporairement au système d'information dans le cadre d'une prestation ou d'un stage, en raison de son annexion aux contrats conclus avec les prestataires et aux conventions de stage.

2 Usage des ressources et règles d'utilisation

2.1 Usage professionnel des ressources

L'utilisation du système d'information du département, notamment la messagerie et internet, est dédié à un usage professionnel.

2.2 Usage personnel des ressources

L'usage à titre personnel du système d'information du département est toléré.

Cet usage doit être raisonnable, conforme aux dispositions légales en vigueur et ne jamais détériorer le service pour les utilisateurs, que ce soit en termes de :

- Volume d'information transmise, stockée ou manipulée : ne pas encombrer les réseaux et espaces mémoires professionnels ;
- Temps d'utilisation ;
- Nature de l'usage.

La pratique du « streaming » (lecture audio/vidéo par Internet) est interdite.

Les espaces de travail utilisés à des fins personnelles ainsi que les courriels personnels doivent clairement porter la mention « PERSO », « PERSONNEL » ou « PRIVE ». Le contenu de ces espaces de travail et messages ne peut être consulté par d'autres personnes (administrateur, hiérarchie...) qu'avec le consentement de l'agent et sous sa supervision.

L'utilisateur est seul responsable de la gestion de ces espaces et courriels. Le département ne peut être tenu responsable de leur détérioration ou disparition.

2.3 Arrivées, changements de postes et départs

2.3.1 Affectations et bon usage des ressources

Les ressources qui vous sont attribuées sont liées à votre affectation.

Les ressources restent la propriété du département. Les affectations sont adaptées, suspendues ou supprimées en fonction des besoins de votre poste. Il est de votre responsabilité de vérifier que les accès dont vous disposez sont strictement nécessaires et suffisants. Si votre travail évolue au sein du département, il est impératif de faire suspendre les accès devenus obsolètes au même titre que vous pouvez demander l'ouverture de nouveaux accès.

Ces attributions sont personnelles, les outils et accès ne doivent pas être prêtés à d'autres personnes.

Vous ne devez jamais partager votre mot de passe.

Un mot de passe est strictement personnel. Il vous identifie sur le réseau et associe systématiquement votre identité à vos actions. Par défaut, vous serez donc responsable de toutes les actions réalisées à l'aide de votre mot de passe.

Vous devez garder en bon état de marche les moyens informatiques qui vous sont affectés, tant d'un point de vue physique que logique.

La DSN maintient et met à jour le système d'information. Vous ne devez pas modifier la configuration des outils ou en empêcher la mise à jour.

Vous ne devez pas introduire ou utiliser de logiciels sans autorisation.

Les logiciels sont installés pour couvrir vos besoins professionnels tout en respectant les licences d'utilisation et la sécurité du système d'information.

Il est interdit de procéder à des copies ou cessions de ces licences, que ce soit à titre gratuit ou onéreux.

Les nouveaux besoins en termes d'application doivent être exprimés auprès de la hiérarchie (ou de la DSN). L'utilisateur veille à indiquer auprès de la DSN les applications qu'il n'utilise plus et ainsi permettre le redéploiement des licences auprès d'autres agents.

Pour les tablettes et smartphones, si vous configurez un compte personnel et/ou installez des logiciels tiers via des magasins d'applications, vérifiez la licence et les droits d'accès que vous accordez aux applications à vos données et à celles du Département (SMS, messages, contacts, agendas, etc.).

Vous ne devez pas stocker sur votre ordinateur les fichiers professionnels.

Les fichiers professionnels nécessitant une sauvegarde doivent être enregistrés sur les outils mis à disposition par la DSN (stockage en ligne à privilégier : la ruche SharePoint pour les documents sensibles, Microsoft Teams pour les documents non-sensibles et la plateforme Adoc - <https://adoc.ille-et-vilaine.fr/> - pour transférer des fichiers à des tiers). Les fichiers personnels ne doivent jamais être stockés sur le réseau du département.

Vous devez être vigilants sur l'utilisation des ordinateurs partagés.

Les ordinateurs partagés sont utilisés par plusieurs utilisateurs. Chaque utilisateur doit être vigilant à supprimer tous les fichiers personnels ou professionnels avant de rendre l'ordinateur.

2.3.2 Départ

L'utilisateur et son encadrement préparent son départ suffisamment à l'avance.

Pour les données professionnelles :

Les données professionnelles contenues sur l'ordinateur ou dans la messagerie doivent être versées sur des espaces de travail partagés. L'utilisateur informera son service de l'emplacement des documents pour garantir la continuité de service. Il mettra également en place un message d'absence pour rediriger les interlocuteurs professionnels et ainsi assurer la continuité de service.

L'utilisateur n'a pas le droit d'emporter de documents professionnels sans autorisation de la collectivité. Toute extraction de données concernant le système d'information, le fonctionnement interne de la collectivité, les agents ou les usagers peut déclencher des poursuites.

Pour les données personnelles :

L'utilisateur prend toutes les précautions pour prévenir ses interlocuteurs « personnels » d'un changement de messagerie. Les dotations informatiques et de communication sont restituées à la collectivité.

L'accès aux ressources informatiques (y compris la messagerie) est suspendu. Au bout d'un certain temps ces ressources seront détruites.

L'utilisateur qui quitte la collectivité est averti qu'il n'aura plus accès à sa messagerie et que les données de celle-ci seront supprimées quelques semaines après son départ.

L'utilisateur qui quitte le département perd ses accès aux ressources informatiques.

En aucun cas, un ancien utilisateur de la collectivité, quel que soit son statut, ne peut accéder à ses anciens équipements, à ses données ou au service de messagerie.

2.3.3 La nécessité de continuité de service

En cas d'absence non prévue de l'utilisateur et afin d'assurer la continuité de service, son supérieur hiérarchique peut demander à la DSN de faciliter :

- La mise en place d'un message d'absence sur la messagerie de l'utilisateur ;
- Le transfert des messages professionnels de l'utilisateur ;
- La récupération des documents professionnels de l'utilisateur sur ses équipements.

Par principe, un accord écrit de l'utilisateur est demandé préalablement à toute action.

Ces opérations se déroulent sous le contrôle d'un collègue de l'utilisateur absent qui s'assure qu'aucun document ou message personnel n'est volontairement ouvert.

Traçabilité de la procédure : La demande d'accès est écrite, motivée et signée par le supérieur hiérarchique. Un compte rendu des opérations est rédigé et signé par les opérateurs.

2.4 Télétravail et mobilités

Pour l'exercice de ses missions professionnelles, l'utilisateur peut devoir emporter des équipements nomades (ordinateurs portables, tablettes, smartphones, etc.) fournis par le département hors des locaux du département.

L'utilisateur est responsable de son matériel professionnel et ne doit pas le laisser sans surveillance, sauf à le laisser, complètement éteint et dans un lieu privatif à accès restreint (domicile ou chambre d'hôtel, par exemple), si possible sous clé.

En cas de perte ou de vol d'un matériel, l'utilisateur doit se rapprocher de la DSN afin de signaler au plus vite l'évènement et valider le besoin ou non de porter plainte.

Lors des connexions au système d'information en mobilité, l'utilisateur doit veiller à préserver la confidentialité de l'ensemble des informations professionnelles (y compris à son domicile).

Il est interdit de se connecter à distance, en dehors de la messagerie, ou d'utiliser les dispositifs de connexion sécurisée fournis par le département à partir d'un équipement non fourni par la collectivité.

Le système d'information du département n'est pas accessible en dehors de la France.

L'utilisateur doit également, autant que possible, éviter les connexions au système d'information à partir d'un réseau public peu sécurisé (hotspot Wifi public, de restaurants, gares, etc.).

Il est rappelé que l'ensemble des documents professionnels doit être stocké sur les espaces dédiés, sécurisés et sauvegardés, et non pas sur les disques durs des postes de travail, non sauvegardés.

2.5 Internet, la messagerie et les réseaux sociaux

Vous n'avez pas accès à l'ensemble du réseau Internet.

Le département met en œuvre un système de filtrage sur l'accès Internet. Les sites sont catégorisés et vous accédez uniquement aux catégories autorisées pour votre profil d'accès à Internet.

Ce filtrage permet :

- De respecter le décret 2015-125 « relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique » ;
- De protéger les mineurs éventuellement présents dans les locaux à l'exposition de contenus à risques ;
- De contrôler la mise à disposition de contenus protégés par le droit d'auteur ;
- De préserver la bande passante pour la consultation de sites utiles dans le cadre professionnel.

Le département garde les journaux d'accès durant une année conformément aux obligations de tout fournisseur d'accès à Internet. Ces traces nominatives permettent de répondre à une réquisition judiciaire ou à une demande de la hiérarchie.

2.5.1 La messagerie

Le contenu des messages est conforme à la loi

Les messages stockés, ou envoyés par un utilisateur ne doivent pas comporter de contenu proscrit par la loi : injurieux, raciste, xénophobe, négationniste, etc.

Si un utilisateur reçoit un tel message, il ne peut en être tenu responsable, mais il est de son devoir de le détruire. Il ne doit donc pas en solliciter l'envoi en participant à des groupes de discussion ou en consultant des sites manipulant de tels contenus.

Conservation des messages

Il est conseillé :

- De conserver les messages ayant un caractère contractuel sur une durée au moins égale à celle du contrat ;
- De détruire rapidement les messages sans valeur, surtout s'ils sont volumineux ;
- De purger régulièrement les messages anciens devenus inutiles (plus de 2 ans).

Le département investit dans les moyens nécessaires à la sauvegarde des messages professionnels.

Pas d'information sensible dans un courrier électronique

Si des informations sensibles doivent être transmises, il convient de solliciter la DSN afin que des outils de transfert sécurisé soient mis en œuvre. Aucune donnée personnelle sensible ne doit être échangée par la messagerie.

Les destinataires sont maîtrisés

Il est conseillé d'utiliser les listes de diffusion avec prudence et de vérifier systématiquement la pertinence des destinataires de la liste : un mail envoyé par erreur ne peut être bloqué.

De même il convient d'être attentif aux homonymes.

Les copies doivent être justifiées par un réel besoin d'en connaître : une surabondance de copies ne fait que saturer les destinataires qui finissent par les classer ou détruire sans en prendre connaissance.

Les messages à risque

La plupart des incidents de sécurité (logiciels-rançons, logiciels espions, attaque virale massive, vol d'information...) commencent avec un mail piégé :

- Soit une pièce jointe contenant le piège ;
- Soit un lien dans le message qui conduit sur un site piégé.

Vous ne devez pas utiliser ou diffuser votre adresse de messagerie professionnelle en dehors de vos activités professionnelles.

L'utilisation de l'adresse de messagerie du département pour utiliser des services en ligne à titre personnel ou sa diffusion sur les réseaux sociaux est interdite.

Ne confondez pas votre activité professionnelle et personnelle sur les réseaux sociaux.

Si vous participez aux réseaux sociaux à titre personnel, restez discret sur vos activités professionnelles et respectez les droits et obligations de tout fonctionnaire (entre autres obligation de réserve, respect du secret professionnel, neutralité et discrétion professionnelle).

Si vous participez aux réseaux sociaux à titre professionnel, c'est en accord avec votre hiérarchie et les services de communication.

2.6 Utilisation de ressources tierces

Un utilisateur peut configurer l'accès à la messagerie du département sur son équipement personnel.

L'utilisateur s'assure d'un bon niveau de sécurité de son périphérique afin de protéger ses données et celles du département. L'assistance du département est sous forme de documentation. Le support n'intervient pas sur des périphériques personnels.

Il est interdit de connecter un équipement personnel au réseau interne du département. Seuls les équipements munis d'une étiquette inventaire peuvent être raccordés à une prise réseau ou au Wi-Fi interne.

Les équipements personnels ou de visiteurs peuvent utiliser le Wi-Fi « invité » qui donne accès à Internet. La loi oblige le département à identifier et tracer les usagers de ces accès.

L'utilisation de supports amovibles, type clé USB, est interdite.

Il est interdit de connecter un périphérique inconnu sur un poste de travail du département.

Les clés USB ne doivent jamais être connectées sur un ordinateur du département. Les périphériques sont connectés sous l'entière responsabilité de l'utilisateur de l'ordinateur.

Seuls certains outils de stockage en ligne sont autorisés par le département.

Pour des documents professionnels, l'usage de services de stockage en ligne « grand public » est rigoureusement interdit par le département. Seuls quelques services sont autorisés pour le partage ou le transfert de documents professionnels.

L'utilisation de toute ressource cloud non validée par le département est interdite. En cas de besoin particulier, une demande doit être adressée à la DSN.

La plupart des services connus ne respectent pas les nombreuses règles applicables en France (code de la santé, CNIL, directives de l'Etat, etc.), ne sont pas suffisamment sécurisés et peuvent être soumis au contrôle de services de renseignements étrangers.

L'utilisateur est entièrement responsable du dépôt et de l'usage des documents stockés en ligne jusqu'à leur retrait. Le stockage en ligne n'est pas un outil d'archivage ; les documents ne restent en ligne que le temps strictement nécessaire.

2.7 Droit à la déconnexion

Tous les agents ont le droit à la déconnexion.

Pour le bien-être de tous, il est demandé aux agents de ne pas envoyer de mail en dehors des heures ouvrées. La messagerie reste accessible le soir et le week-end pour répondre à des besoins exceptionnels. En cas d'urgence, le téléphone ou le face à face est plus efficace et une moindre source de stress. Chez lui et hors du cadre d'astreinte, l'agent peut éteindre ses équipements et n'est pas obligé de répondre aux sollicitations avant sa reprise de service.

2.8 Responsabilité des utilisateurs

L'utilisateur doit :

- Verrouiller son poste de travail en cas d'absence et garder les documents papiers confidentiels sous clé ;
- Assurer la protection des données auxquelles il accède en utilisant les différents moyens de sécurité mis à sa disposition en particulier les systèmes de sauvegarde ;
- Veiller à la confidentialité des informations et des secrets (en particulier les mots de passe) qu'il peut être amené à connaître dans le cadre de son activité ;
- S'engager à ne pas mettre à la disposition d'utilisateurs non autorisés un accès au système d'information du département par un moyen quelconque ;
- Signaler tout événement ou incident de sécurité qu'il peut constater (vol de matériel, fuite de données...), à sa hiérarchie et à la DSN via la plateforme d'assistance numérique @telier (<https://atelier.ille-et-vilaine.fr/>) ou en cas d'incident grave directement au DSN ou au chargé de mission gestion des risques numériques de la DSN;
- Signaler toute violation ou toute tentative de violation de son compte à sa hiérarchie et à la DSN ;
- Veiller, lors de l'installation de logiciel, au respect de la propriété intellectuelle et des procédures internes vis à vis des codes malicieux ;
- Faire preuve de la plus grande correction et discrétion à l'égard de ses interlocuteurs dans les échanges et notamment pour les courriers, forums de discussions, *etc.* ;
- Faire preuve de discernement dans l'usage de la messagerie tant sur le plan du contenu que des destinataires afin d'éviter toute situation préjudiciable au département ;
- S'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, diffamatoire, pédophile.

L'utilisateur ne doit pas :

- Installer ou faire installer de logiciel n'ayant pas de rapport direct avec l'activité professionnelle ;
- Tenter d'outrepasser ses droits d'utilisation des logiciels mis à sa disposition ;
- Utiliser ou tenter d'utiliser des comptes de tiers sans autorisation explicite de la hiérarchie ;
- Connecter des ressources tierces (supports amovibles, ordinateur personnel, *etc.*) au système d'information du département ;
- Donner des renseignements sur le système d'information du département à une personne extérieure sans y être autorisé par ses missions et sa hiérarchie, et sans nécessité avérée ;

- Exprimer des opinions ou déclarations au nom du département, ou susceptibles d'être comprises comme exprimées au nom du département sur les réseaux sociaux sans autorisation expresse ;
- Emettre, faire suivre, conserver ou plus généralement traiter des messages dont le contenu ou les pièces attachées constitueraient ou comporteraient une méconnaissance des dispositions légales ou réglementaires ou qui causeraient ou seraient susceptibles de causer un dommage, notamment aux intérêts du département, des agents ou usagers ;
- Se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Laisser sans surveillance des documents confidentiels ;
- Consulter des sites internet ou stocker des documents, des données ou des images, portant atteinte à la dignité des personnes, à caractère pédophile ou pornographique, et plus généralement toute donnée à caractère illégal.

3 Protection de la vie privée

3.1 Traitement des données personnelles

Les exigences légales et réglementaires en vigueur (notamment le RGPD) définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés. Depuis 2006, le département est doté d'un agent qui vous conseille et vous accompagne sur la mise en œuvre et l'usage des fichiers contenant des données nominatives.

Ces traitements doivent respecter les cinq grands principes des règles de protection des données personnelles dont chaque utilisateur doit avoir connaissance :

- Le **principe de finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- Le **principe de proportionnalité et de pertinence** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- Le **principe d'une durée de conservation limitée** : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
- Le **principe de sécurité et de confidentialité** : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- Les **droits des personnes**.

Il est en particulier interdit de :

- Mettre en place des fichiers sans information du DPO ;
- Consigner des informations sensibles ou sans rapport avec la finalité du fichier ;
- Détourner l'usage d'un fichier ;
- Conserver des données obsolètes.

Tout fichier doit être suffisamment sécurisé. Les personnes faisant partie du fichier doivent être informées de son existence et de leurs droits.

Tout traitement doit être déclaré auprès du DPO du département.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer un traitement de données à caractère personnel, il doit auparavant en avoir fait la demande auprès de sa hiérarchie et du DPO du département, afin que le département puisse en gérer la conformité.

Le département a pris les mesures nécessaires afin que les traitements contenant des données à caractère personnel soient enregistrés dans le registre des activités de traitement.

Il est rappelé aux utilisateurs que les informations collectées et traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

Protection particulière des données sensibles

La collecte et le traitement des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, état de santé ou vie sexuelle, données génétiques, biométriques) est par principe interdit sauf exception. De même certaines

données font l'objet d'une protection particulière (numéro de sécurité sociale, infraction et condamnations) et leur traitement est strictement encadré.

Chaque utilisateur s'engage à ne traiter ces données que dans le cadre des obligations légales en vigueur et à faire preuve de vigilances quant aux mesures de protection à mettre en œuvre.

Utilisation des zones de commentaires

Chaque utilisateur s'engage à ne pas mentionner des informations qui porteraient atteinte aux droits des personnes concernées et à n'inscrire que des commentaires objectifs.

Respect du droit à l'image

Vous ne pouvez pas reproduire l'image d'une personne sans en avoir une autorisation écrite. Les agents comme les usagers ont le droit de décider si leur visage peut être reproduit sur un site ou une publication.

Respect des droits d'auteur

De nombreux documents (textes, illustrations, images, sons, films, etc.) sont soumis à des droits d'auteur et ne peuvent pas être librement utilisés.

3.2 Confidentialité des données personnelles

L'accès par l'utilisateur aux informations et documents conservés sur les systèmes d'information doit être limité à ceux qui lui sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre délibérément 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.

Marquage des documents.

Les documents « Publics », « Internes » ou « Confidentiels » doivent être marqués comme tels sur chaque page.

Gestion des documents sensibles.

Les documents « internes » ou « confidentiels » ne doivent pas être laissés sans surveillance lors de l'impression.

Si vous trouvez un document (salle de réunion, imprimante, fax) rappez-le à son propriétaire ou, si vous ne pouvez pas identifier le propriétaire, détruisez-le.

Si vous êtes destinataire d'un message par erreur, avertissez l'émetteur.

3.3 Contrôles automatisés

Le système d'information du département s'appuie sur des journaux (fichiers « log »), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur des serveurs et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations du département, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Tout utilisateur pourra avoir accès aux données le concernant en faisant une demande formelle auprès du DPO du département. Ces données ne seront conservées que dans les conditions applicables par la réglementation en vigueur.

4 Mesures de contrôle de l'utilisation des ressources

Pour des nécessités de maintenance, de gestion technique et de sécurité, l'utilisation des ressources du système d'information, ainsi que les échanges via le réseau, peuvent être analysés et contrôlés dans le respect de la législation applicable notamment de la loi sur l'informatique et les libertés et des règles d'utilisation énoncées dans la présente charte.

Des analyses des fichiers « log » de ces ressources sont effectuées pour répondre à des besoins de sécurité, pour détecter des comportements à caractères frauduleux, et de détection des comportements abusifs qui pourront donner lieu à des investigations supplémentaires dans les limites de la réglementation.

Le système d'information garde de nombreuses traces d'utilisations.

Pour les besoins de la justice, notamment pour la poursuite d'infractions pénales, le département doit conserver certaines données pendant un délai d'un an.

Par exemple, les relevés des accès à internet et les relevés d'appels passés depuis un téléphone (fixe ou mobile) sont conservés une année et mis à disposition en cas de réquisition ou de contrôle. Ils peuvent être conservés plus longtemps en cas d'incident grave (procédure de séquestre).

Le système d'information peut fournir des statistiques.

Ces rapports anonymes permettent de quantifier les usages et adapter le système d'information. Ils sont conçus pour ne pas identifier l'utilisateur.

Une consultation de l'usage des outils informatiques et de communication peut être demandée pour des motifs légitimes.

Par souci de transparence, cette demande est immédiatement portée à la connaissance de l'utilisateur. De même, le rapport est porté aussi bien à la connaissance de l'utilisateur que de son supérieur hiérarchique.

Il sera avant tout statistique avec des éléments de comparaison :

- Internet : métriques et sites internet consultés (nom de domaine uniquement) ;
- Messagerie : métriques ;
- Téléphonie : métriques et 6 premiers chiffres des numéros appelés.

Rappel : Les métriques d'usage d'un système d'information ne constituent pas un outil de management.

5 Charte administrateur

Par nature, chaque système, solution ou service, possède des comptes à hauts privilèges qui permettent d'en assurer l'administration. Ces comptes sont attribués de manière strictement personnelle à des utilisateurs particuliers, nommément désignés : les administrateurs.

Les administrateurs du système d'information ont la charge de la mise en place et du maintien du bon fonctionnement du système d'information.

Les interventions des administrateurs se caractérisent par l'accès aux ressources au travers d'un **profil utilisateur à hauts privilèges**, à savoir le profil dit « administrateur », qui leur permet d'accéder à la plupart des données des systèmes qu'il gère. De ce fait, un administrateur doit assurer la confidentialité et la robustesse de son propre mot de passe en se conformant aux règles en vigueur.

L'administrateur ne communique pas son mot de passe à autrui, le manquement à cette règle engage sa propre responsabilité vis-à-vis des actions effectuées avec son identifiant par une autre personne.

De plus, les obligations de confidentialité dévolues ici aux administrateurs, s'imposent également à tous les agents de la DSN ainsi qu'aux correspondants et référents qui, au cours de leur mission, viendraient ponctuellement à accéder aux informations des usagers de la collectivité et des utilisateurs du système d'information.

Les administrateurs respectent les mesures de sécurité définies par le département et ne cherchent pas à les contourner, en particulier, ils ne désactivent pas les mécanismes de traçabilité ni ne portent atteinte à l'intégrité des fichiers de journalisation qui permettent de définir les actions qui leur sont imputables.

Tout constat de contournement de cette règle serait constitutif d'une faute grave.

Le non-respect des règles de la charte peut entraîner la responsabilité des administrateurs internes ou externes au département et, le cas échéant, les exposer à des sanctions proportionnelles à la gravité des faits.

5.1 Principes généraux à respecter

5.1.1 Principe de finalité et de maîtrise des droits

Dans le cadre de leurs fonctions, les administrateurs utilisent un compte individuel et pourvu des privilèges d'administration. Ce compte assure l'imputabilité de leurs actions sur les ressources.

L'administrateur assure la traçabilité de son travail afin de lier toutes ses actions à une demande écrite ou au traitement d'un incident enregistré, surtout celles concernant des données utilisateurs ou usagers.

Il est interdit à l'administrateur de faire usage de ces droits à d'autres fins que celles de ses missions.

En cas de besoin de créer un compte générique ou fonctionnel (ex. compte de service), le responsable hiérarchique ou fonctionnel valide obligatoirement le bien-fondé de cette demande et définit les limites de l'autorisation ainsi délivrée.

Lorsque l'utilisation de droits particuliers n'est pas nécessaire, l'administrateur s'identifie sur le système d'information avec un profil « utilisateur ».

5.1.2 Principe de confidentialité

Les administrateurs sont tenus à un **devoir de discrétion professionnelle** pour toutes les données, informations ou documents dont ils ont connaissance dans l'exercice de leurs fonctions, y compris les données « métier », quelles qu'elles soient.

Dans le cadre de ses fonctions, l'administrateur a connaissance de certaines données techniques (exemple : architecture du SI, plan d'adressage IP, etc.) pouvant faciliter les tentatives d'intrusion dans le système d'information. L'administrateur doit en respecter strictement le caractère confidentiel.

L'administrateur ne doit pas chercher à connaître les mots de passe des utilisateurs. S'il doit, dans l'exercice de ses fonctions, réinitialiser un mot de passe, il doit utiliser les procédures de la DSN et en informer l'intéressé sans délai à la suite de l'opération.

Les administrateurs observent en particulier l'obligation de confidentialité qui protège spécifiquement certaines catégories de données. Ceci recouvre les données « personnelles » marquées « PRIVE, PERSO ou PERSONNEL », ainsi que les données « à caractère personnel » pour lesquelles le principe de sécurité et de confidentialité doit être respecté.

Les administrateurs sont tenus d'alerter directement le DPO en cas de doute ou s'ils constatent un dysfonctionnement sur le traitement de ces données.

Concernant les données dites « personnelles », et sauf disposition législative particulière en ce sens (ex. obligation de dénonciation de crimes ou délits ou cas de requête judiciaire), les administrateurs ne peuvent en aucun cas, y compris à l'égard des échelons hiérarchiques supérieurs, être contraints de divulguer des informations protégées qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions.

En cas de demande d'accès ou de communication d'informations adressée directement à l'administrateur et portant sur des traitements de données à caractère personnel, l'administrateur vérifie au préalable la qualité du demandeur en tant que « destinataire » ou « tiers autorisés » auprès du responsable de traitement ou du DPO.

Cette demande est obligatoirement motivée et écrite. L'administrateur ne peut mener ce type d'opérations de son propre chef.

5.1.3 Principe de moindre gêne et d'information des utilisateurs

Lorsque l'intervention de l'administrateur peut avoir une influence sur le service rendu par un système, il doit intégrer les contraintes opérationnelles et avertir les utilisateurs, par le moyen le plus approprié avec préavis et informations (conséquences, date et heure de début et de fin prévue de l'intervention).

Dans tous les cas, l'administrateur qui doit interrompre tout ou partie du service rendu aux utilisateurs doit :

- Informer clairement les utilisateurs ;
- Limiter la gêne occasionnée en réduisant autant que possible la durée et la fréquence de ces interruptions et en choisissant des plages horaires adaptées ;
- Indiquer aux utilisateurs les moyens de supporter ces perturbations s'il y en a.

Dans le cas particulier de l'utilisation de logiciels de télémaintenance qui permettent une action à distance du poste de travail d'un utilisateur, toute précaution doit être prise afin de garantir la transparence de l'emploi de ces outils.

En particulier l'administrateur doit :

- Avant toute intervention, informer et recueillir l'accord de l'utilisateur pour pouvoir « prendre la main » sur son poste ; assurer la traçabilité des opérations de maintenance ;
- Accéder aux seules données nécessaires à l'accomplissement de sa mission ;
- Demander à l'utilisateur de rester observer son intervention (ne pas quitter son poste de travail pendant l'intervention).

Dans les circonstances exceptionnelles d'un incident de sécurité d'une particulière gravité, le besoin d'une réaction rapide peut amener l'administrateur à accéder au poste de travail d'un utilisateur sans son accord mais dans le respect des règles de protection des données personnelles.

Enfin, dans les cas de **mobilité** (interne comme externe) d'un utilisateur, les administrateurs mandatés veillent et contribuent à la fermeture technique des comptes informatiques de l'utilisateur et à la destruction de ses données personnelles à l'issue de son départ. Si besoin, ils remettent à son successeur toutes les données électroniques (fichiers, mails...) non identifiées comme personnelles nécessaires à la continuité de sa mission.

5.2 La surveillance et le contrôle

Les administrateurs ont la charge de la sécurité et de la surveillance du système d'information.

Les finalités de ces missions sont notamment :

- La protection des activités du département et de ses intérêts économiques, financiers et sociaux ainsi que l'ensemble des informations qui y sont rattachées ;
- La protection du système d'information vis-à-vis des agissements illicites d'utilisateurs ;
- La vérification de l'application des principes et règles définis dans la présente charte.

L'administrateur n'effectue que des contrôles prévus dans le cadre de ses activités ou pour lesquels il a reçu une demande formelle de sa hiérarchie.

Dans le cas où les dispositifs de surveillance recueillent des données personnelles, leur mise en œuvre se fait dans le respect des règles de protection des données personnelles établies dans cette charte (Cf. 3).

Nota : les traitements statistiques (débits, volumes, fréquence, etc.) permettant de dégager des moyennes portant sur l'utilisation des ressources (et non sur l'analyse des contenus) se révèlent le plus souvent suffisants pour détecter des usages abusifs.

Dans le cadre de sa mission, l'administrateur peut avoir accès à des informations relatives aux administrés ou agents. Le principe de confidentialité des données s'applique.

Si les données sont présumées « à caractère professionnel », l'administrateur peut opérer et reporter, à tout moment et hors la présence des utilisateurs, toute opération de contrôle nécessaire à sa mission.

Si les données sont présumées « personnelles » (marquées « PRIVE », « PERSO » ou « PERSONNEL »), l'administrateur ne peut y avoir accès que dans le cadre du traitement d'un incident.

Dans le cas où l'administrateur se trouve en présence de données à caractère manifestement « personnelles », mais non libellées comme telles par l'utilisateur, aucune faute ne peut être retenue contre lui ou contre le département. Le principe de respect de la vie privée et de confidentialité des données s'applique toutefois à ces données.

5.3 Le traitement des dysfonctionnements et incidents de sécurité

Dans le cadre de leurs fonctions, les administrateurs peuvent être alertés sur des dysfonctionnements ou des incidents de sécurité touchants les systèmes d'information (SI) :

- Les dysfonctionnements regroupent toutes les défaillances physiques ou logiques rencontrées sur un système, voire sur les servitudes indispensables à son bon fonctionnement (énergie, climatisation...), ainsi que la dégradation des performances ou capacités des systèmes ;
- Les incidents de sécurité regroupent tous les faits ou événements volontaires ou involontaires, issus d'un utilisateur légitime ou non, voire d'un système externe, et portant atteinte à la sécurité du système administré, au respect de la loi ou aux intérêts du département.

Un administrateur constatant un dysfonctionnement réagit selon les consignes propres au système concerné et prend immédiatement les mesures permettant de :

- Faire cesser la défaillance actuelle (ainsi que ses éventuels effets ultérieurs) en cohérence avec le besoin opérationnel qui reste prioritaire ;
- Recouvrer le niveau nominal de fonctionnement et de sécurité du système ;
- Assurer la continuité de service, au besoin en mode dégradé.

Dans le cas du constat d'un incident de sécurité, l'administrateur établit un **rapport d'incident** qui est communiqué sans délai au Directeur des Systèmes Numériques (DSN), à son adjoint et au chargé de mission gestion des risques numériques de la DSN. En cas de violation de données personnelles, le DPO est informé et s'assure de la déclaration à la CNIL dans les 72 heures.

Il fournit une copie à son responsable hiérarchique. Suivant la nature des faits rapportés et les suites envisagées, les destinataires peuvent demander à l'administrateur d'identifier nommément le ou les utilisateurs concernés.

5.3.1 Contrôle et manipulation des données personnelles dans le cadre d'un incident

Lorsque des données personnelles sont concernées par le rapport d'incident, l'administrateur s'attache alors à spécifier uniquement leur caractère présumé illicite ou abusif sans en révéler précisément le contenu (ex. : présence d'un logiciel contrefait, vidéos personnelles, etc.).

Un rapport d'incident peut être suivi :

- Soit d'une simple mise en garde de(s) l'utilisateur(s) concerné(s) par le Directeur des Systèmes Numériques (DSN), son adjoint ou le responsable hiérarchique ;
- Soit, en raison de la gravité des faits ou de la violation répétée des règles précisées dans la charte être signalé par le Directeur des Systèmes Numériques (DSN) auprès du responsable de la Direction des Ressources Humaines (DRH) qui décide, en concertation avec le responsable de la « Direction Assemblée, Affaires Juridiques et Documentation », des suites données au dossier.

Cette décision peut conduire notamment à :

1. Un dépôt de plainte :

Cette situation s'applique en particulier dans le cas de crimes ou délits constatés entrant notamment dans le domaine du « manifestement illicite » à savoir, tel que défini par la jurisprudence, notamment :

- Atteintes aux mineurs (pornographie enfantine) ;
- Incitation à la haine ou à la violence raciale ;
- Atteintes à la dignité humaine ;
- Apologie de crimes de guerres ou de crimes contre l'humanité ;
- Contenus racistes, antisémites, négationnistes ou révisionnistes.

Dans ce cas, le responsable de la Direction des Ressources Humaines ou de la « Direction Assemblée, Affaires Juridiques et Documentation », préparateur de la mesure de dépôt de plainte qui sera signée par le président ou son représentant, valide et transmet à l'administrateur les requêtes officielles l'obligeant en particulier à remettre à l'autorité judiciaire (magistrat ou officier de police judiciaire destinataire de la requête) toute information susceptible d'intéresser l'enquête – y compris les données personnelles de l'utilisateur.

2. Des investigations techniques complémentaires :

Ces investigations ont pour seul objet de conforter la qualification des faits constatés et la nature ou le niveau des mesures et sanctions appropriées.

Dans ce cas, le responsable de la Direction des Ressources Humaines est seule habilitée à solliciter la DSN afin que l'administrateur, auteur du rapport d'incident initial, procède à une investigation ciblée plus approfondie pouvant se rapporter aux données « personnelles » de l'utilisateur.

Dans ce cas, l'administrateur respecte les prescriptions fixées par la jurisprudence qui exigent :

1. Soit la présence de l'utilisateur ;
2. Soit, à défaut de la présence de l'utilisateur :
 - Que celui-ci ait été contacté par l'administrateur ou sa hiérarchie pour l'inviter à être présent, par tous moyens appropriés ;
 - Que le département puisse justifier d'un cas de force majeure c'est-à-dire d'un risque ou évènement particulier portant atteinte à la sécurité de son SI et présentant à la fois un caractère d'urgence et de gravité certain.

L'ensemble des éléments recueillis dans ce cadre sont consignés dans le rapport d'incident.

Note : la présence ou l'information préalable de l'utilisateur n'implique pas nécessairement l'accord de ce dernier.

En tout état de cause, l'administrateur et les différents responsables impliqués dans la procédure de gestion des incidents de sécurité agissent avec la plus grande discrétion et respectent à tout moment le principe de présomption d'innocence.

5.3.2 La préservation des preuves

Un incident pouvant déboucher sur des poursuites disciplinaires ou judiciaires, toutes les mesures adaptées, afin de préserver les éléments de preuve des faits constatés, doivent alors être prises.

Dans ce cadre et suivant la nature des enjeux et la complexité des procédures et systèmes concernés, la DSN peut décider de confier la responsabilité de la collecte des éléments de preuve à un tiers compétent offrant par ailleurs des garanties d'impartialité et de neutralité de son action.

Afin de fixer la preuve dans le temps et éviter sa disparition ou son altération, l'administrateur respecte les précautions conformes à l'état de l'art en matière de sécurité et d'*inforensique*.

Ainsi lorsqu'il intervient en particulier dans le cadre d'un incident de sécurité en cours d'instruction, l'administrateur doit agir rapidement afin de :

- Déconnecter, en cohérence avec les besoins opérationnels, le serveur, l'élément de stockage ou le poste client du réseau afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte du délit ;
- Eviter, dans la mesure du possible, d'éteindre l'équipement « incriminé » (cette opération pouvant causer l'effacement des traces présentes en mémoire) ; si la machine doit cependant être éteinte, le choix de la méthode d'extinction du système (débranchement du cordon d'alimentation ou procédure ordinaire d'arrêt système) s'opérera suivant les paramètres suivants : l'ordre de volatilité des informations, leur priorité dans les investigations et l'impact des opérations sur les données ciblées ;
- Ne pas connecter de supports amovibles (ce qui génèrerait des traces perturbatrices dans les journaux) ;
- Restreindre l'accès physique et logique à la ressource « incriminée » afin que personne ne modifie sa configuration avant l'intervention des services compétents ;
- Le cas échéant, verrouiller le(s) compte(s) du (des) Utilisateur(s) mis en cause, ainsi que l'accès aux comptes de messagerie et en informer les personnes concernées.

L'administrateur assure une traçabilité et un historique de son intervention. Il documente dans un registre des interventions (« journal de bord ») l'ensemble des constatations faites et des actions effectuées tant sur les systèmes que sur les données, en précisant notamment :

- Les dates et heures (heure système du poste et heure GMT « réelle ») ;
- Le nom des fichiers ou commandes exécutés ainsi que les login et mot de passe utilisés si des actions d'administration sont nécessaires.

L'administrateur assure l'intégrité des données collectées par tout moyen approprié (calcul d'une empreinte (hash) par exemple) et préserve les informations pertinentes pouvant compléter et appuyer ses constatations telles que : supports de sauvegardes récentes et journaux d'évènements.

6 Sanctions

La loi et les textes réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques (articles 226-16 à 226-24 du Code pénal portant sur les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, articles 323-1 à 232-7 du Code pénal portant sur les atteintes aux systèmes de traitement automatisé de données).

Il est rappelé qu'en cas d'atteinte à l'un des principes protégés par la loi, la responsabilité administrative, pénale et/ou civile de l'utilisateur ainsi que celle de la collectivité est susceptible d'être recherchée.

Par ailleurs, le non-respect des règles définies dans cette charte peut entraîner une sanction disciplinaire.

Compte-tenu de son objet, la présente charte s'applique à l'ensemble des personnes utilisant le système d'information du département (agents de la fonction publique, salariés de droit privé, stagiaires, personnes en contrat d'apprentissage, intervenants extérieurs, élus, etc.), qu'elle soit liée ou non par un contrat de travail avec celui-ci.

Toutefois, la procédure disciplinaire et les sanctions relèvent de l'entreprise d'origine des intérimaires ou des intervenants extérieurs.

7 Textes de référence

D'une façon générale, l'utilisation du système d'information doit s'effectuer dans le respect des lois, des règlements, et des usages. Chaque utilisateur veillera à ne pas nuire aux droits et intérêts d'autrui.

La loi informatiques et libertés de 1978 – modifiée en 2004 et 2019 - et le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 ou RGPD (règlement général sur la protection des données) définissent les obligations faites aux responsables de traitements et les droits qu'ont les personnes concernées par le traitement.

La Loi n° 2004-575 du 21 juin 2004 **pour la confiance dans l'économie numérique** (LCEN) définit :

- Les obligations faites aux **éditeurs de contenus**.
- Les obligations faites aux **hébergeurs de contenus**.
- Les obligations faites aux **fournisseurs d'accès** à Internet.
- Les obligations relatives à la **prospéction** par fax, SMS, téléphone ou messagerie.

Elle est complétée par le Code des Postes et des Communications Electroniques ainsi que par la Loi Informatique et Libertés.

Le Code de la Propriété Intellectuelle dispose dans ses articles L 331-1 et suivants que toute **reproduction ou diffusion d'une « œuvre de l'esprit »** (image, son, film, photo, logiciel, structure d'une base de données, contenu « sui generis » d'une base de données, *etc.*) sans l'autorisation préalable de son auteur constitue une contrefaçon, passible de poursuites civiles ou de poursuites pénales.

Le Code pénal protège les systèmes informatiques du **piratage ou de la fraude**. Cette partie du Code Pénal définit les atteintes aux systèmes de traitement automatisé de données : accès ou maintien frauduleux dans un système, actes visant à fausser ou entraver son fonctionnement, méfaits dans les interventions, sur les données.