Ces conditions seront appréciées comme étant caractérisées et réunies au cas par cas pour chaque marché et titulaire de marché. Dans l'affirmative, le cas de force majeure entraîne l'obligation pour l'acheteur public soit d'accorder un report de délai au titulaire et de l'exonérer des pénalités de retard, soit de résilier le marché.

* * * * *

Ainsi, il est demandé aux acheteurs publics du Pays d'appliquer dans un esprit équitable et solidaire les dispositions en faveur des entreprises, évoquées dans la présente circulaire, visant à faciliter la bonne exécution des contrats publics malgré la pénurie et la hausse de certaines matières premières ou composants indispensables à la réalisation de leurs prestations.

L'application de ces dispositions doit toutefois toujours être justifiée par des éléments objectifs et étayés.

Je vous prie de prendre les dispositions nécessaires à l'application de ces préconisations.

Fait à Papeete, le 29 septembre 2021.
Edouard FRITCH.

CIRCULAIRE n° 7726 PR du 1er octobre 2021 relative à la charte informatique applicable aux services administratifs, aux ministères, à la vice-présidence et à la présidence de la Polynésie française

Le Président de la Polynésie française,

A : M. le vice-président, Mmes et MM. les ministres, Mmes et MM. les chefs des services administratifs de la Polynésie française,

Mesdames, Messieurs,

La présente circulaire définit la charte informatique applicable aux services administratifs, aux Ministères, à la Vice-Présidence et à la Présidence de la Polynésie française. Elle pose les modalités d'utilisation et d'administration des moyens informatiques et des outils numériques dans ces entités.

Elle participe au bon fonctionnement des systèmes d'information en favorisant l'adoption de bonnes pratiques et l'utilisation adaptée des ressources. Elle contribue à assurer la sécurité et la protection des données de l'Administration.

Elle est applicable à toute personne physique, dénommée « *utilisateur* », à qui l'usage d'outils numériques est consenti par l'Administration, quel que soit le statut de cette personne (agent ou prestataire de service) et quel que soit le lieu d'utilisation des outils mis à sa disposition.

Elle est également applicable à toute personne physique, dénommée « *administrateur* », intervenant avec certains privilèges sur les outils numériques du système d'information de l'Administration, quel que soit le statut de cette personne (agent ou prestataire de service).

On entend par « *outils numériques* » l'ensemble des équipements informatiques (serveurs, réseaux, ordinateur fixe ou PC, ordinateur portable, scanner, imprimante, téléphone mobile, tablette, disque dur, clé USB, etc.), des moyens de communication (messagerie, accès Internet, etc.), des logiciels et applications et des bases de données, mis à disposition de l'utilisateur.

L'usage des outils numériques par les représentants syndicaux fait l'objet de dispositions spécifiques.

Les usages non conformes aux dispositions de la présente charte peuvent être regardés comme des fautes professionnelles susceptibles d'entraîner pour l'utilisateur ou l'administrateur, une suspension conservatoire des outils mis à disposition, des sanctions disciplinaires, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

Les prescriptions de cette charte peuvent être précisées ou complétées en tant que de besoin par des dispositions spécifiques à certains services ou secteurs d'activité.

La présente charte s'applique immédiatement et pourra être révisée en fonction des évolutions technologiques et des impératifs de sécurité.

Sommaire

I – PRINCIPES GENERAUX

1. CADRE JURIDIQUE APPLICABLE

Le cadre juridique applicable fait l'objet de l'annexe 1 à la présente charte.

2. MISE A DISPOSITION DES OUTILS NUMERIQUES

Sur demande d'une autorité hiérarchique habilitée, les outils numériques sont mis à disposition de l'utilisateur, par le service de l'informatique de la Polynésie française (SIPf).

Les modalités de remise et de retrait des équipements par le SIPf ainsi que les consignes liées à leur utilisation font l'objet de l'annexe 2.

3. SERVICES PLACES EN DEHORS DU PERIMETRE DU SIPF

Lorsqu'un service ne relève pas du périmètre du SIPf, les outils sont mis à disposition de l'utilisateur par le service informatique dont il dépend. Ce service informatique exerce à son égard l'ensemble des missions confiées au SIPf par la présente charte.

4. USAGE PROFESSIONNEL DES OUTILS NUMERIQUES

Les outils numériques mis à disposition de l'utilisateur par l'Administration sont destinés à un usage professionnel.

Un usage privé est toléré à condition qu'il soit raisonnable dans sa fréquence et dans sa durée, qu'il soit licite et qu'il n'affecte pas la sécurité et le fonctionnement normal des services.

Un usage raisonnable s'entend d'un usage ponctuel et de courte durée, assimilable à un temps de pause au travail.

Par défaut, les usages et contenus sont réputés professionnels ; seuls les espaces, répertoires, fichiers et/ou messages qualifiés expressément, de « *privés* » « *personnels* » ou « *confidentiels* » seront considérés comme tels. Ces contenus « *privés* », « *personnels* » ou « *confidentiels* » ne peuvent pas être enregistrés sur les espaces de stockage partagés. Ils doivent obligatoirement être stockés sur le poste de travail de l'utilisateur.

En toutes circonstances, y compris pour un usage privé, l'utilisation des outils numériques ne doit pas porter préjudice à l'administration ni atteinte à son image. L'utilisation doit être conforme à l'ordre public et aux bonnes mœurs. Il est notamment interdit de consulter des sites ou contenus de nature pornographique, terroriste….

L'usage privé des ressources informatiques peut être restreint par l'Administration, notamment dans un souci de bon usage (sécurité, performance...).

En cas d'usage inapproprié au regard de la présente charte, l'agent peut voir suspendu ou retiré tout ou partie des moyens informatiques mis à sa disposition et peut voir restreints ses droits d'accès aux systèmes. Il pourra également faire l'objet d'une procédure disciplinaire, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

5. CONTROLE DES USAGES

L'Administration met en œuvre des dispositifs de contrôle et de surveillance afin :

- d'assurer la sécurité des systèmes d'information ;
- de permettre l'emploi des outils dans des conditions optimales ;
- de s'assurer que les usages privés restent raisonnables ;
- de répondre aux exigences légales.

Ces mesures peuvent prendre la forme :

- de dispositifs de gestion des droits d'accès et des habilitations des utilisateurs ;

- de contrôles visant à la détection de virus ou logiciels malveillants, la prévention contre l'usurpation d'identité, la lutte contre les messages non sollicités, la prévention contre la fuite, la perte d'informations ou la suppression des comptes inutilisés ;

- d'une surveillance, par le biais d'interceptions, des canaux de communication, dans des cas spécifiques ;

- de dispositifs de collecte de données et de traces notamment pour :
  - les services de messagerie (messagerie électronique, sms, messagerie instantanée)[1] ;
  - l'accès à internet[2] ;
  - l'usage des moyens d'impression et de reprographie ;
  - les actions réalisées par les utilisateurs dans certaines applications ou services[3].

Ces dispositifs sont mis en œuvre conformément au cadre légal et réglementaire en vigueur. L'utilisateur a notamment un droit d'accès et de rectification aux données qui le concernent.

En cas de détection ou de présomption d'anomalies, d'incidents de sécurité ou d'utilisation non conforme des outils, des actions de contrôle peuvent être exercées manuellement par les administrateurs, notamment en vue de l'identification d'un fait fautif et de son auteur.

Les données, même si elles relèvent de la tolérance d'usage privé, peuvent être communiquées aux autorités habilitées par la loi disposant d'un droit de communication sur ces données, notamment à l'autorité judiciaire qui en ferait la demande.

---

[1] identifiants, émetteur, nombre, volumétrie, fréquence d'envoi ou de réception, présence de pièces jointes (nature, volume, identification), classification, notamment entre privé et professionnel lorsque la mention est disponible

[2] historique complet de navigation, volumétrie, durée, identifiant de l'utilisateur, adresse IP, protocoles utilisés

[3] identifiants des équipements, utilisateurs, ressources et données, nature, date et volume des flux de connexion.

6. MODALITES D'UTILISATION DES OUTILS NUMERIQUES DANS LE CADRE DU TELETRAVAIL, DU TRAVAIL A DISTANCE OU DU TRAVAIL A DOMICILE

Les modalités particulières d'utilisation des outils numériques dans le cadre du télétravail, travail à distance ou travail à domicile sont fixées par note du Chef du service de l'informatique, sans préjudice des règles fixées dans la présente charte et des prescriptions éventuellement édictées par les services.

Elles sont portées à la connaissance des personnels concernés qui sont tenus de s'y conformer.

7. DROITS DE L'UTILISATEUR

L'utilisateur bénéficie des droits au respect de sa vie privée, au secret de ses correspondances privées et à la protection de ses données personnelles dans les conditions prévues par la législation applicable rappelée en annexe 1 de la présente charte.

8. USAGE DES OUTILS NUMERIQUES DANS LE CADRE SYNDICAL

L'utilisateur peut faire usage des outils numériques pour les activités syndicales exercées au bénéfice des personnels de l'Administration, dans le respect des dispositions applicables à ces activités. Il peut notamment utiliser les équipements mis à sa disposition (ordinateurs, messagerie…) pour exercer son mandat syndical au profit des agents publics et correspondre avec les personnels dans la défense de leurs intérêts.

9. DEVOIRS DE L'UTILISATEUR

L'utilisateur veille à faire un usage des outils numériques conforme à ses obligations générales de réserve, probité, neutralité, secret et discrétion professionnels. Notamment, il lui est interdit de tenir des propos contraires à l'ordre public, diffamatoires, racistes, homophobes, ou constituant une diffusion de fausse nouvelle.

L'utilisateur ne peut pas utiliser les outils numériques à des fins personnelles, au-delà de la tolérance prévue par la présente charte.

Il veille à la bonne protection des données de l'Administration et plus particulièrement des données à caractère personnel qu'il traite ou auxquelles il a accès dans l'exercice de ses fonctions.

Notamment, il veille à ne pas les divulguer à des personnes non autorisées ou n'ayant pas le besoin d'en connaître.

Il les conserve sur les espaces de stockage partagés et sauvegardés de son service. Il ne peut en faire de copie sur un support externe que sous réserve de l'accord de sa hiérarchie et à la condition que ce support présente des garanties de sécurité suffisantes (chiffrement…). Il lui est interdit d'héberger des données professionnelles sur ses équipements personnels (clés USB, téléphone...) ou sur des moyens personnels de stockage en ligne.

Il ne doit pas procéder à la destruction de données professionnelles ou les altérer ni sciemment les rendre inaccessibles, notamment en cas d'absence, de départ ou de changement d'affectation.

L'utilisateur ne doit pas accéder ou tenter d'accéder à des données pour lesquelles il ne dispose pas d'habilitations.

Il veille à protéger les données de tout accès illégitime et prend, à son niveau, toute mesure destinée à éviter que les données soient lues, copiées, altérées ou détruites par des tiers non autorisés.

L'utilisateur respecte les consignes et mesures de sécurité informatique et de protection des données personnelles mises en place par le SIPf ou la déléguée à la protection des données et participe aux actions de sensibilisation proposées.

Il signale sans délai au service informatique toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.

L'utilisateur prend soin du matériel mis à sa disposition et veille à en éviter le vol, la perte ou la dégradation. Il utilise les outils informatiques mis à sa disposition de façon responsable et raisonnée, par exemple, en évitant des envois et impressions inutiles, en éteignant l'alimentation du poste de travail lorsqu'il le quitte.

Les différents cas d'application de la charte et les obligations de l'utilisateur qu'ils induisent sont précisés à l'annexe 3.

10. ACCES AUX DONNEES DE L'UTILISATEUR

Les données professionnelles détenues par l'utilisateur doivent demeurer accessibles à sa hiérarchie. L'utilisateur veille donc à les stocker sur les espaces de stockage partagés et sauvegardés.

A défaut et dans tous les cas où les nécessités de service l'exigent, les administrateurs peuvent, sur demande écrite du Chef de service et en présence de l'utilisateur, accéder manuellement aux données professionnelles de ce dernier. La demande écrite émane du directeur de cabinet, lorsqu'elle concerne les personnels des cabinets des membres du Gouvernement.

En cas d'absence de l'utilisateur, ce dernier en est dûment informé par tout moyen et au plus tard lorsqu'il reprend ses fonctions.

L'accès aux fichiers qualifiés expressément de « *privés* », « *personnels* » ou « *confidentiels* » n'est pas autorisée, sauf si ces fichiers compromettent le bon fonctionnement et la sécurité des systèmes d'information. Dans ce cas, les administrateurs interviennent dans les conditions prévues au point 3 du II ci-après.

11. CAS PARTICULIER DES DONNEES SENSIBLES

Dans certains services détenant des données sensibles[4], ou d'autres données qui justifient une protection particulière[5], des règles spécifiques peuvent être instaurées (chiffrement des données, modalités de sauvegarde ou de stockage…). Lorsqu'il traite de telles données, l'utilisateur est tenu de se conformer strictement aux règles ainsi édictées.

II- REGLES APPLICABLES AUX ADMINISTRATEURS

1. DEFINITION ET RÔLE DES ADMINISTRATEURS

L'administrateur réseau est chargé de la gestion du réseau qui comprend tous les comptes et équipements du réseau informatique (switchs, routeurs, modems, pare-feu, proxy, connectivité réseau, VPN, accès aux réseaux…).

L'administrateur système est responsable des serveurs dont il gère l'installation, le paramétrage, le maintien, l'évolution, la sauvegarde, la restauration, la supervision et le support. L'administrateur des postes de travail assure l'ensemble de ces activités sur les postes de travail.

Le gestionnaire ou administrateur de base de données (DBA) est responsable du bon fonctionnement des serveurs de bases de données tant dans la conception des bases, que des tests de validation, de l'exploitation, de la protection et du contrôle d'utilisation.

Le gestionnaire d'application est responsable d'une ou plusieurs applications. Il contribue au fonctionnement, à l'amélioration de la performance de l'application et participe à sa gestion courante et à son évolution.

Le gestionnaire des accès utilisateurs aux serveurs de fichiers est le responsable des accès sur le serveur de fichiers. Il attribue ou retire les droits d'accès utilisateurs sur les dossiers et/ou fichiers.

2. DROITS D'ACCES PRIVILEGIES

Les administrateurs interviennent, avec certains privilèges, dans le fonctionnement des systèmes d'information et mettent en œuvre des outils de supervision technique.

L'administrateur dispose de droits d'accès privilégiés aux informations relatives aux utilisateurs. Il en use dans le respect strict de la finalité de ses missions et des prérogatives que lui confère la présente charte.

Il attribue, modifie ou supprime les accès des utilisateurs dans le cadre des procédures définies par le service informatique ou, le cas échéant, les responsables des services.

---

[4] Données qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

[5] Par exemple, données révélant la précarité, la situation de handicap, la situation économique…des personnes concernées ou des données présentant un intérêt stratégique pour l'administration.

3. ACCES AUX DONNEES

Pour assurer le bon fonctionnement et la sécurité des systèmes d'information, l'administrateur prend toute mesure jugée utile. Il peut accéder aux données enregistrées par l'utilisateur.

L'accès aux fichiers qualifiés expressément de « *privés* », « *personnels* » ou « *confidentiels* » n'est autorisé que s'il n'existe pas d'autre moyen moins intrusif et si les fichiers compromettent le bon fonctionnement et la sécurité des systèmes d'information.

L'accès aux données par l'administrateur se fait en présence de l'utilisateur. En cas d'urgence ou en cas d'absence de l'utilisateur, ce dernier en est dûment informé par tout moyen et au plus tard lorsqu'il reprend ses fonctions.

L'administrateur est tenu à une obligation de confidentialité sur ces données. Il ne peut pas être contraint de les divulguer, sauf disposition législative particulière en ce sens, notamment dans le cadre d'une demande d'autorités dûment habilitées (autorités judiciaires notamment) ou en application des articles 434-1, 434-3, 223-6 et 226-14 du code pénal.

Toutefois, l'administrateur peut communiquer ces informations à sa hiérarchie, dans le respect de la vie privée de l'utilisateur, si ces données font peser un risque avéré sur les systèmes d'information ou leur sécurité.

4. UTILISATION DES LOGICIELS DE PRISE DE MAIN A DISTANCE

Les logiciels de prise de main à distance peuvent notamment permettre à l'administrateur d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

Les actions de télémaintenance ne peuvent pas être détournées pour contrôler ou surveiller l'activité de l'utilisateur sur son poste de travail.

L'administrateur veille à prendre toute précaution utile pour garantir la transparence dans l'emploi des logiciels de prise de main à distance et la confidentialité des données auxquelles il accède par ce moyen (information préalable et recueil de l'accord de l'utilisateur avant l'intervention sur son poste ; intervention réalisée en présence de l'utilisateur dans toute la mesure du possible ; traçabilité des opérations de maintenance).

5. GESTION DES TRACES INFORMATIQUES

L'administrateur gère les traces informatiques à l'aide de mécanismes de journalisation afin de s'assurer du bon fonctionnement et de la sécurité du système d'information.

Il accède aux journaux informatiques[6] dans le seul but de diagnostiquer les dysfonctionnements ou les incidents de sécurité affectant ces systèmes.

Il garantit l'intégrité, la disponibilité et la confidentialité de ces journaux jusqu'à leur date légale de destruction.

Dans tous les cas où les nécessités de service l'imposent, les administrateurs peuvent, à la demande du responsable hiérarchique et après que les utilisateurs concernés en aient été dûment informés, transmettre des informations des journaux, sans que ces informations ne puissent servir à la surveillance des agents.

6. INFORMATION ET ALERTE

L'administrateur informe sa hiérarchie et le responsable de la sécurité du système d'information de toute infraction et des incidents de sécurité dont il a connaissance. Lorsqu'ils affectent des données à caractère personnel, il en informe le délégué à la protection des données.

L'administrateur signale à sa hiérarchie tout usage non conforme ou abusif des ressources informatiques mises à disposition des utilisateurs : surcharge de la bande passante, téléchargements massifs, saturation des espaces disques partagés...

Fait à Papeete, le 1er octobre 2021.
Edouard FRITCH.

---

[6] Fichier comportant les enregistrements, dans l'ordre chronologique, des évènements sur un serveur, une base de données, une application....

ANNEXE 1

CADRE JURIDIQUE APPLICABLE

Le cadre juridique applicable est constitué des réglementations relatives :

- à la protection des données à caractère personnel fixée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que le règlement européen UE 2016-679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) ;

- à la dématérialisation des actes des autorités administratives et aux téléservices prévue par la loi du pays n° 2017-30 du 2 novembre 2017 et les arrêtés pris pour son application et notamment l'arrêté n° 2043 CM du 18 octobre 2018 fixant le référentiel général de sécurité ;

- à l'accès aux documents administratifs posé par la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'améliorations des relations entre l'administration et le public ainsi que le code des relations entre l'administration et le public, dans leurs dispositions applicables à l'administration de la Polynésie française ;

- aux droits et obligations des fonctionnaires prévus par le statut général de la fonction publique de la Polynésie française défini par la délibération n° 95-215 du 14 décembre 1995 et ses textes subséquents ;

- aux droits et obligations des agents non fonctionnaires de l'administration de la Polynésie française prévus par le code du travail de la Polynésie française et la convention collective des ANFA du 10 mai 1968 ;

- à l'obligation de collecte de traces sur internet au titre des articles L 34-1 et R10-13 du code des postes et télécommunications électroniques applicables en Polynésie française ;

- au respect du droit d'auteur conformément au code de la propriété intellectuelle de la Polynésie française ;

- au droit au respect de la vie privée et au droit au respect de la personne tel que prévus par les articles 9 et 16 du code civil ;

- au respect de l'intimité de la vie privée (droit à l'image, paroles) tel que prévu et sanctionné par les articles 226-1 et 226-2 du code pénal ;

- au secret des correspondances émises par la voie des communications électroniques, tel que posé dans l'article 226-15 du code pénal.

ANNEXE 2

MODALITES DE REMISE ET DE RETRAIT DES EQUIPEMENTS PAR LE SERVICE DE L'INFORMATIQUE ET PRECAUTIONS D'UTILISATION

Dans le cadre de ses missions, le SIPf dote les agents de l'Administration d'un poste de travail standard composé d'une unité centrale, d'un clavier, d'une souris et d'un écran. Les autres types de poste de travail (portable ou station de travail) doivent être justifiés pour des usages en rapport avec la fonction de l'agent.

1. Demande et livraison de matériels

   La demande est exprimée par un formulaire mis à disposition par le SIPf. La demande est obligatoirement signée par le Chef de service (ou par le directeur de cabinet, pour ce qui concerne les cabinets des membres du Gouvernement).

2. Précautions d'utilisation

   Les services doivent équiper les postes de travail d'un onduleur fonctionnel ou disposer d'un réseau électrique ondulé.

   L'utilisateur veille à éteindre l'alimentation électrique, chaque soir, en quittant son poste.

   Il évite toute obstruction des aérations des appareils et ne place pas d'objets lourds sur ces derniers.

   Il prend soin des équipements qui lui sont fournis. Il veille à éviter toute chute d'objet ou de liquide susceptible de les endommager.

3. Retrait des matériels

   Lorsque l'utilisateur quitte son service (fin de contrat, mutation…) le matériel doit être restitué au SIPf. Ce dernier est contacté à cet effet et procède à son enlèvement. Le Chef de service (ou le directeur de cabinet s'il s'agit de personnels de cabinet) donne toute instruction qu'il juge utile sur le sort des données présentes dans le PC (transfert sur le serveur de fichiers, suppression…).

Les dispositions de la présente annexe peuvent être précisées ou complétées par le SIPf en tant que de besoin.

ANNEXE 3

CAS D'APPLICATION DE LA CHARTE

1. POSTES DE TRAVAIL ET TERMINAUX MOBILES

Un ordinateur est fourni à l'utilisateur par le SIPf.

Pour certains besoins spécifiques, l'utilisateur peut se voir attribuer d'autres matériels par son service (onduleur, tablette, smartphone, clef USB, disque externe…).

L'utilisateur ne doit pas en modifier les paramétrages techniques et de sécurité ni empêcher les mises à jour des matériels et/ou logiciels informatiques qui lui sont remis.

L'installation de logiciels ou applications qui ne sont pas fournis par le SIPf nécessite l'autorisation préalable du SIPf qui s'assure de leur compatibilité avec les équipements et de l'absence de risque de sécurité.

La connexion au réseau professionnel ou l'utilisation d'équipements qui ne sont pas fournis par le SIPf ou qui n'ont pas fait l'objet d'un contrôle par ce dernier, n'est pas autorisée.

Les matériels sont réservés à l'activité professionnelle. Ils ne peuvent pas être confiés ou prêtés à un tiers, notamment pour ce qui concerne les ordinateurs portables ou les tablettes.

L'utilisateur ne doit pas faire preuve de négligence en laissant son matériel sans surveillance, en particulier dans les locaux administratifs facilement accessibles ou à l'extérieur de ces derniers. Il doit s'assurer de verrouiller sa session lorsqu'il s'éloigne de son poste de travail.

De manière générale, l'utilisateur doit être vigilant et se conformer aux consignes de sécurité définies par son service ou le SIPf, s'il stocke des données sensibles sur ses équipements nomades (ordinateur portable…).

L'utilisateur efface régulièrement de ces équipements, les données non utiles qui y sont stockées.

L'utilisateur doit déclarer sans délai toute perte ou tout vol d'un matériel à son supérieur hiérarchique et/ou au SIPf, selon le cas.

L'utilisateur facilite l'accès à son poste de travail aux personnels du SIPf chargés de la maintenance des matériels et logiciels. Il doit fermer les applications informatiques et les fichiers ouverts sur le poste, notamment les documents sensibles ou confidentiels, avant toute intervention d'un agent du SIPf. Enfin, il s'assure que la session de prise en main à distance est fermée en fin d'intervention.

En mobilité (wifi ou autres), les accès aux réseaux de l'Administration ne sont autorisés que via des logiciels fournis par l'administration, par exemple par l'emploi d'un VPN (virtual private network)

2. MESSAGERIE ELECTRONIQUE

La messagerie électronique fournie par l'Administration est réservée à l'activité professionnelle.

L'utilisateur en fait un usage raisonné et veille à ne pas surcharger les boîtes de messagerie. Notamment, il procède, à intervalles réguliers, à l'archivage ou la suppression des messages devenus inutiles.

Un usage privé de la messagerie est toléré dans les conditions prévues au point 4 du I de la présente charte. Seuls les messages qualifiés expressément de « *privés* », « *personnels* » ou « *confidentiels* » seront considérés comme tels.

Dans son usage de la messagerie, il est interdit à l'utilisateur de masquer sa véritable identité, ou usurper l'identité d'autrui.

Tout message électronique envoyé depuis la messagerie professionnelle engage non seulement la responsabilité et l'image de l'utilisateur mais aussi celle de l'Administration. La messagerie ne peut donc pas servir à diffuser des messages de type canulars (hoax), chaînes, escroquerie par hameçonnage (phishing), jeux, paris, ni être utilisée sur des sites internet (groupes de discussion (chats), commerce, forums, blogs, etc…), sans rapport avec l'activité professionnelle.

Une messagerie personnelle ne doit pas être utilisée dans un contexte professionnel. En conséquence, les messages professionnels reçus sur la messagerie professionnelle ne doivent pas être redirigés manuellement ou automatiquement vers une messagerie personnelle.

Lors d'envois de données, en particulier sensibles, l'utilisateur s'assure que la liste des destinataires du message ne comporte pas de destinataire inapproprié.

L'utilisateur ne doit pas ouvrir les messages douteux, les pièces jointes suspectes, ni répondre à l'émetteur de ces messages ou cliquer sur les liens qui y sont présents.

Il prévient le SIPf en cas de doute, par tous moyens.

Les services traitant des données sensibles peuvent recourir à des messageries sécurisées et en imposer l'usage à l'utilisateur. Dans de tels cas, l'utilisateur applique strictement les consignes d'utilisation émanant de sa hiérarchie ou du SIPf.

La création d'une liste de diffusion[7] (exemples : secretariat@service.gov.pf, direction@service.gov.pf...) peut être réalisée par le SIPf, à la demande du Chef de service. Ce dernier veille à garantir la mise à jour régulière de ses utilisateurs, afin qu'elle corresponde à l'organisation et la répartition des fonctions.

Dans tous les cas, tout envoi d'un message depuis une adresse associée à une liste de diffusion doit permettre d'assurer l'identification de l'expéditeur d'un courriel.

---

[7] Adresse électronique unique qui permet l'envoi d'un mail à différents utilisateurs.

Pour des raisons de sécurité, la création de comptes génériques[8] n'est pas autorisée.

3. IDENTIFIANTS ET MOTS DE PASSE

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

Un utilisateur ne doit pas communiquer ses moyens d'authentification, notamment ses mots de passe, à un tiers. Sa responsabilité peut être engagée pour les actions réalisées avec ses mots de passe, sur les serveurs, applications ou systèmes.

Un utilisateur ne doit pas utiliser les moyens d'authentification d'un tiers. S'il en prend connaissance de manière fortuite, il doit en informer immédiatement le titulaire afin que ce dernier les modifie.

Les mots de passe choisis doivent être suffisamment robustes (combinaison de lettres en minuscules, majuscules, chiffres, caractères spéciaux, et sans lien évident avec l'utilisateur).

Ils ne doivent pas être affichés sur papier ou support numérique et ne doivent pas être partagés. L'utilisateur ne doit pas s'envoyer par courriel ses propres mots de passe. Les mots de passe doivent être modifiés régulièrement.

Les identifiants et mots de passe professionnels doivent être utilisés uniquement dans le cadre professionnel. Les mots de passe à usage privé ne doivent pas être utilisés dans le cadre professionnel.

4. HABILITATION DES UTILISATEURS

Chaque Chef de service détermine les accès aux ressources informatiques (réseaux, applications, serveurs…) dont bénéficient les personnels placés sous sa responsabilité, au regard des fonctions et besoins de chacun. Il veille à l'adéquation de ces habilitations à l'organisation du service et à leur réactualisation aussi souvent que nécessaire. Elles sont donc modifiées en cas d'évolution ou de changement dans la fonction de l'utilisateur.

Les droits d'accès et habilitations sont répertoriés dans un document, tenu à jour sous l'autorité du chef de service. Ce document est communiqué, en cas de besoin, à la demande du SIpf, du responsable de la sécurité des systèmes d'information ou de la Déléguée à la protection des données.

5. ACCES A INTERNET

Sauf contrainte particulière, l'accès des agents à internet est autorisé, à la demande du Chef de service, notamment pour leur permettre d'assurer au mieux leur mission.

Afin d'assurer le respect des obligations qui lui incombent, l'Administration met en place :

---

[8] Compte disposant d'un identifiant et d'un mot de passe partagés entre plusieurs utilisateurs.

- des dispositifs de filtrage des accès à internet, qui limitent l'accès aux seules catégories de sites autorisées ;
- des mécanismes de collecte des informations de connexion des utilisateurs à internet.

Les restrictions d'accès à internet peuvent être levées lorsque certains besoins métiers d'un utilisateur le justifient, sur demande du Chef de service concerné ou du directeur de cabinet (par exemple pour un accès à Youtube ou facebook…).

L'accès à internet est réservé à l'usage professionnel. Un usage privé, ponctuel, est toléré dans les limites prévues au point 4 du I de la présente charte.

6. SERVICES ACCESSIBLES DEPUIS UN POSTE DE TRAVAIL NON PROFESSIONNEL

L'Administration peut mettre à disposition de l'utilisateur des services en accès public depuis un poste de travail non professionnel (webmail, applications professionnelles…).

Dans ce cas, elle peut mettre en place des contrôles visant à assurer la traçabilité de l'appareil utilisé pour la connexion et la sécurité du système d'information (antivirus présent, logiciels mis à jour régulièrement,).

L'utilisateur ne doit pas enregistrer ses identifiants et mots de passe sur le navigateur d'un poste non professionnel. Il veille à se déconnecter et supprimer en fin de session les données issues du service consulté (ex : historique des cookies et fichiers professionnels téléchargés depuis le service)

L'utilisateur n'est pas autorisé à accéder au service depuis un poste de travail public (type cybercafé).

7. RESEAUX SOCIAUX « GRAND PUBLIC »

Dans le cadre professionnel et notamment pour les besoins de la communication institutionnelle, un utilisateur peut être amené à utiliser les réseaux sociaux « grand public » (Facebook, Youtube, Linkedin, Instagram…). Il les utilise dans les limites et conditions fixées par sa hiérarchie.

En dehors de ces hypothèses, l'utilisation des réseaux sociaux « grand public » au moyen des outils numériques mis à sa disposition par l'Administration n'est pas autorisée et aucune donnée professionnelle ne peut y être transférée.

Dans son utilisation privée de ces réseaux sociaux, l'utilisateur respecte son obligation de réserve et veille à ne pas porter atteinte à la réputation et l'image de l'Administration.

8. TELECHARGEMENT ET STREAMING

Le téléchargement de fichiers (notamment de films ou de musique) ainsi que l'accès aux ressources en streaming qui ne sont pas justifiés par les fonctions de l'utilisateur, sont interdits.

Le téléchargement de certains fichiers volumineux ou présentant un risque pour la sécurité des systèmes d'information (virus, codes malveillants, programmes espions…) ou l'accès à certaines ressources en streaming peuvent être limités ou interdits.

L'utilisateur doit faire preuve de vigilance lorsqu'il télécharge un fichier provenant d'une source non professionnelle. Par exemple, il vérifie que le site est sécurisé en https (cadenas) dans la barre de navigation de son navigateur internet.

9. STOCKAGE ET PARTAGE SUR INTERNET

L'utilisation de services de stockage et partage sur internet doit être autorisée par le Chef de service. L'utilisateur veille à recourir à des outils présentant toutes les garanties de sécurité et de conformité aux règles de protection des données personnelles. Il déclare ces utilisations à la D*éléguée à la protection des données.

Le SIPF peut recommander certains services. Dans ce cas, l'utilisateur recourt de manière privilégiée à ces outils.

10. VISITEURS ET PRESTATAIRES

Les personnes extérieures à l'Administration telles que les visiteurs, stagiaires, intervenants, prestataires, ne doivent pas avoir accès au système d'information sans l'accord préalable du Chef de service et du service informatique. Tout accès doit être octroyé dans des conditions permettant de garantir la sécurité des données de l'Administration.

Les intervenants extérieurs doivent s'engager au respect de la présente charte par eux-mêmes, leurs personnels et éventuels sous-traitants. Tout contrat signé avec un prestataire ayant accès aux données, aux programmes informatiques ou autres moyens, doit impérativement comporter des clauses précisant la nature et la durée de l'accès octroyé, les obligations auxquelles le prestataire est tenu, ainsi que des clauses encadrant le traitement des données à caractère personnel, lorsque de telles données sont concernées.