'Âmuitahira'a nō te mau 'oire
SPCPF
SYNDICAT POUR LA PROMOTION DES COMMUNES DE POLYNÉSIE FRANÇAISE

REPUBLIQUE FRANÇAISE

Liberté – Egalité – Fraternité

Délibération n° 06/2024/SPC

du 23 janvier 2024

relative à la charte informatique du SPCPF

LE COMITE SYNDICAL DU SPCPF

En sa séance du 23 janvier 2024 à 08h00, convoqué par le président du SPCPF par lettre n° 11/2024/SPC du 12 janvier 2024,

Sous la présidence de Monsieur Cyril TETUANUI, Madame Françoise AH SCHA, étant secrétaire de séance ;

Le nombre de délégués en exercice étant de 92, il a été constaté le quorum avec les 61 membres présents et 5 procurations ;

Membres présents

Archipel	Collectivité	Nom	Prénom	Statut
Australes	Rapa	NARII	Tuanainai	Titulaire
Australes	Rapa	TEIPOARII épse RIARIA	Annette	Suppléant
Australes	Rurutu	ITAE TETAA	James, Tihoti	Suppléant
Australes	Rurutu	DEGAGE	Mereaine	Suppléant
Australes	Tubuai	TAHIATA	Fernand	Titulaire
Australes	Tubuai	VIRIAMU	Tihina	Titulaire
Iles du Vent	Mahina	TEUIRA	Damas	Titulaire
Iles du Vent	Mahina	FRITCH	Edgar	Titulaire
Iles du Vent	Moorea-Maiao	HAUMANI	Evans	Titulaire
Iles du Vent	Moorea-Maiao	TEARIKI	Ronald	Titulaire
Iles du Vent	Moorea-Maiao	YOU SING	Jade	Suppléant
Iles du Vent	Paea	TEHEI	Teddy	Titulaire
Iles du Vent	Paea	MARUAE	Andréa	Suppléant
Iles du Vent	Papara	TAAE	Sonia	Titulaire
Iles du Vent	Papeete	TEMEHARO	René	Titulaire
Iles du Vent	Pirae	LECHENE	Eliane	Suppléant
Iles du Vent	Pirae	FRITCH	Edouard	Titulaire
Iles du Vent	Punaauia	TIRAO	Aldo	Suppléant
Iles du Vent	Punaauia	LISSANT	Simplicio	Titulaire
Iles du Vent	Punaauia	PUCHON	Cathy	Titulaire
Iles du Vent	Taiarapu Est	VIVISH	Titaua	Titulaire
Iles du Vent	Teva I Uta	BERNARDINO	Namoeata	Titulaire
Iles du Vent	Teva I Uta	ALPHA	Tearii Te Moana	Titulaire
Iles sous le Vent	Bora-Bora	TCHE épse MAIARII	Nelia	Titulaire
Iles sous le Vent	Huahine	TUMARAE	Grégoire	Suppléant
Iles sous le Vent	Huahine	LISAN	Marcelin	Titulaire
Iles sous le Vent	Maupiti	UTAHIA épse ATUAHIVA	Alice	Suppléant
Iles sous le Vent	Maupiti	RAUFAUORE	Woullingson	Titulaire
Iles sous le Vent	Taputapuatea	SANQUER épse GOUPIL	Juliana	Titulaire
Iles sous le Vent	Taputapuatea	MOUTAME	Thomas	Titulaire
Iles sous le Vent	Tumaraa	TETUANUI	Cyril	Titulaire
Iles sous le Vent	Uturoa	TAPUTUARAI	Judex	Titulaire
Marquises	Fatu Hiva	TUIEINUI	Henri	Titulaire

Marquises	Nuku Hiva	KAUTAI	Benoit	Titulaire
Marquises	Nuku Hiva	AH SCHA	Françoise	Titulaire
Marquises	Ua Huka	OHU	Nestor	Titulaire
Marquises	Ua Huka	AUNOA	Ranka	Titulaire
Marquises	Ua Pou	CANDELOT	Ady	Titulaire
Tuamotu-Gambier	Anaa	MATAI	Maima	Titulaire
Tuamotu-Gambier	Anaa	HAPII	Basile	Suppléant
Tuamotu-Gambier	Arutua	TAPUTUARAI	Reupena	Titulaire
Tuamotu-Gambier	Fakarava	MARO	Etienne	Titulaire
Tuamotu-Gambier	Fakarava	TOROHIA	Tautahi	Titulaire
Tuamotu-Gambier	Fangatau	NUI	Clément	Titulaire
Tuamotu-Gambier	Gambier	GOODING	Vai Vianello	Titulaire
Tuamotu-Gambier	Hao	BUTCHER épse FERRY	Yseult	Titulaire
Tuamotu-Gambier	Hao	MAI-TAKAMOANA épse APA	Mauricette	Titulaire
Tuamotu-Gambier	Hikueru	TEAMO	Rémy	Titulaire
Tuamotu-Gambier	Hikueru	TEKURIO	Tavahikura	Titulaire
Tuamotu-Gambier	Makemo	TARAHU	Cécile	Titulaire
Tuamotu-Gambier	Manihi	MATA	Judy	Titulaire
Tuamotu-Gambier	Manihi	DROLLET	John	Titulaire
Tuamotu-Gambier	Nukutavake	APA	Roland	Titulaire
Tuamotu-Gambier	Nukutavake	TAGIHIA	Silvano	Titulaire
Tuamotu-Gambier	Rangiroa	MARAEURA	Tahuhu	Titulaire
Tuamotu-Gambier	Reao	LENOIR	Matatini	Titulaire
Tuamotu-Gambier	Tatakoto	HATUUKU	Louis	Titulaire
Tuamotu-Gambier	Tatakoto	TEAGAI	Ernest	Titulaire
Tuamotu-Gambier	Tureia	MATA	Vaiarii	Suppléant
Tuamotu-Gambier	Tureia	BRANDER	Vaitiare	Titulaire
Tuamotu-Gambier	Tureia	BRANDER	Tevahineheipua	Titulaire

Procurations

Archipel	Commune	Prénom Nom	Procuration à
Iles du Vent	Papeete	Jules IENFA	René TEMEHARO
Iles sous le Vent	Bora Bora	Gaston TONG SANG	Nélia TCHE épse MAIARII
Iles sous le Vent	Tumaraa	Pierre TERAIHAROA	Cyril TETUANUI
Iles-sous-le-Vent	Tahaa	Patricia AMARU	Namoeata BERNARDINO
Tuamotu-Gambier	Fangatau	André DIAZ	Clément NUI

Présents : 61
Procurations : 5
Votants : 66
Abstention : 0
Vote pour : 66
Vote contre : 0

Vu la loi organique n° 2004-192 du 27 février 2004 modifiée, portant statut d'autonomie de la Polynésie française, ensemble la loi n° 2004-193 du 27 février 2004, complétant le statut d'autonomie de la Polynésie française ;

Vu le code général des collectivités territoriales applicables aux communes de la Polynésie française, à leurs groupements et à leurs établissements publics dans sa version applicable à la Polynésie française

Vu l'arrêté n° 3453 MAT du 5 février 1980 modifié portant création d'un « syndicat pour la promotion des communes de Polynésie française » ;

EXPOSE DES MOTIFS

Le Syndicat pour la Promotion des Communes en Polynésie Française (SPCPF) met à disposition des utilisateurs les équipements informatiques et les outils de communication nécessaires à l'exercice de leurs fonctions, que ce soit au sein des locaux du SPCPF ou à distance. L'utilisation de ces ressources numériques implique que chaque « Utilisateur » respecte des directives visant à garantir un niveau optimal de sécurité, de confidentialité, de performance, ainsi que la conformité avec les dispositions légales et réglementaires en vigueur. La fiabilité et la sécurité de son système d'information sont une préoccupation centrale du SPCPF, mais elles relèvent également de la responsabilité individuelle de chaque utilisateur.

ADOPTE :

Article 1 : La charte informatique du SPCPF est adoptée. Elle s'applique à tous les utilisateurs du SPCPF, telle que mentionnée dans la charte informatique.

Article 2 : Ce document est amené à évoluer ou être complété en fonction de l'évolution de l'organisation de la structure, des technologies numériques ou des textes.

Article 3 : Conformément aux dispositions de l'article R421-1 du code de justice administrative, le tribunal administratif de Polynésie française peut être saisi par la voie du recours formé contre la présente décision, dans un délai de deux mois à compter de sa publication. La juridiction administrative compétente peut être aussi saisie par l'application de « télé recours citoyen » accessible depuis le site www.telerecours.fr.

Article 4 : Le Président de l'exécution de la présente délibération qui sera publiée et communiquée partout où besoin sera.

Le Président	Le secrétaire de séance
SYNDICAT POUR LA PROMOTION DES COMMUNES POLYNÉSIE FRANÇAISE – République Française Le Président Cyril TETUANUI	Françoise AH SCHA

Publié le : 25/01/2024 Transmis à la subdivision administrative le : 25/01/2024

RF
Haut-Commissariat de Papeete

Contrôle de légalité
Date de réception de l'AR: 25/01/2024
987-200015154-20240123-DEL_06BIS_2024-AR

CHARTE INFORMATIQUE

'Āmuitahira'a nō te mau 'oire

SPCPF

SYNDICAT POUR LA PROMOTION DES COMMUNES DE POLYNÉSIE FRANÇAISE

Référent(s)
Direction générale Département informatique : Responsable du département informatique adjointe / Référent des systèmes d'informations RSSI

Documents Ressources
Recommandations de sécurité relatives aux mots de passe de l'Agence Nationale de la Sécurité des Systèmes d'Information 10 conseils pour la sécurité de votre système d'information du 12 octobre 2009 de la CNIL 9 règles de base pour mieux protéger l'informatique de votre entreprise du CLUSIR Tahiti Le guide de l'hygiène informatique
Documents Annexes
La PSSI du SPCPF Charte administrateur Le livret technique Attestation de lecture de la Charte Informatique Formulaire de demande de dérogation à la charte informatique Note d'information à l'attention des Utilisateurs de l'outil informatique

Charte applicable à compter du	**du rendu exécutoire de la délibération n°03/2024/SPC du 23 janvier 2024**

HISTORIQUE DES MISES A JOUR DU DOCUMENT

Ce document a été créé puis mis à jour par les rédacteurs suivants

Version	Date	Motif	Rédacteur	Validateur
V1	18/07/2023	Travaux de la feuille de route du RSSI	Vaea NAUTA	Ivana SURDACKI
V2	02/08/2023	Questions sur la validation de la charte	Vaea NAUTA	Ivana SURDACKI

SOMMAIRE

I) LETTRE DE LA DIRECTION GENERALE

L'informatique est omniprésente dans notre quotidien. Cet outil est devenu indispensable pour mener à bien nos missions et nous sommes dépendant de son bon fonctionnement. Notre système d'information est également devenu un facteur stratégique pour le développement du SPCPF. L'information que nous manipulons au quotidien a de la valeur. Elle permet de mieux gérer nos activités et les services rendus à nos communes adhérentes. Ce patrimoine informationnel doit être protégé de toute altération ou détournement.

Le SPCPF doit répondre aux nouvelles législations qui exigent un certain niveau de sécurité pour le système d'information du SPCPF. Le règlement général pour la protection des données (RGPD) oblige tout organisme public manipulant des données à caractère personnel à sécuriser ses traitements d'information. Le référentiel général de sécurité (RGS) impose également la mise en place d'une organisation pour identifier les risques numériques afin de les maitriser.

Au-delà du respect de la réglementation, le SPCPF doit donc être exemplaire sur ces sujets s'il souhaite accompagner les communes dans leur modernisation. La digitalisation de nos métiers et la mise en place de nouveaux e-service aux citoyens ne pourront se faire que si la sécurité est maitrisée.

En conséquence, le SPCPF adopte sa charte informatique qui définit les règles d'usages et les droits de chaque agent. Ce document sera complété par une série de bonnes pratiques pour gérer et protéger notre système d'information.

Il est important que chacun comprenne qu'il a un rôle à jouer dans la sécurité du système d'information. Nous sommes tous responsables de la bonne utilisation des moyens informatiques et, à ce titre, nous sommes tous acteurs de la sécurité du système d'information du SPCPF.

II) APPROCHE GENERALE

II.1) Préambule

Le Syndicat pour la promotion des communes en Polynésie française (SPCPF) met à la disposition des Utilisateurs des moyens informatiques et de communication électronique nécessaire à l'accomplissement de leurs missions au sein des locaux du SPCPF ou à distance.

L'utilisation de ces moyens, suppose le respect, par chaque Utilisateur, de règles destinées à assurer un niveau optimum de sécurité, de confidentialité, de performance et, de manière générale, le respect des dispositions légales et réglementaires applicables.

La fiabilité ainsi que la sécurité de notre système d'information sont l'affaire du SPCPF mais également de la responsabilité de chaque Utilisateur.

La présente **charte informatique** est un code de déontologie qui a pour objectifs :

- De sensibiliser les Utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;
- D'informer les Utilisateurs sur :
  - Les usages permis des moyens informatiques mis à leur disposition ;
  - Les règles de sécurité qu'ils doivent suivre ;
  - Les mesures de contrôle prises par le département informatique (DI) ;
  - Les sanctions encourues par les Utilisateurs ;
- De formaliser les règles générales de sécurité que les Utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi déterminer les droits et les devoirs des Utilisateurs.

II.2) Champ d'application

II.2.1) Utilisateurs concernés

La présente charte s'applique à l'ensemble des Utilisateurs du système d'information, tel que :

- Le personnel du SPCPF, tous statuts confondus
- Les stagiaires étudiants
- Le personnel temporaire du SPCPF

Dès l'entrée en vigueur de la présente charte, chaque Utilisateur recevra un exemplaire dont il devra prendre connaissance. Une attestation de lecture de la charte informatique du SPCPF est annexée au présent document. L'Utilisateur devra la remplir, la dater et la signer suivi de la mention « lu et approuvée ».

II.2.2) Périmètre du système d'information

Le système d'information du SPCPF est composé de toutes les ressources matérielles et logicielles qui visent à collecter, classifier, stocker, gérer et diffuser des informations au sein du SPCPF et avec ses partenaires.

II.3) Dérogation possible

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente charte, doit être présentée par écrit au responsable de la sécurité des systèmes d'information (RSSI). Un formulaire de demande de dérogation est annexé à la présente charte informatique. La décision finale sera prise en concertation avec la direction générale, qui se réserve le droit de refuser ou d'accepter les demandes de dérogation.

II.4) Opposabilité

La présente charte est contraignante. Sa valeur juridique est conforme aux dispositions règlementaires en vigueur.

Tout manquement à la présente charte informatique, selon sa gravité, est susceptible de donner lieu à des sanctions disciplinaires fixées par la règlementation en vigueur (FPC), et ce, sans exclusion d'éventuelles actions pénales ou civiles à son encontre.

L'Utilisateur pourra, en outre, voir ses droits d'accès aux ressources et au système d'information et de communication suspendus ou supprimés, partiellement ou totalement.

III) GESTION DES DONNEES PERSONNELLES DE L'UTILISATEUR

III.1) Différenciation entre utilisations professionnelle et personnelle (ou privée)

Les moyens informatiques et de communication électronique, mis à disposition des Utilisateurs sont réservés à un usage professionnel exclusif. Toutefois, l'utilisation, à des fins personnelles, du système d'information du SPCPF, est **tolérée**, dans les limites définies par la présente charte.

En toute hypothèse, l'utilisation des moyens informatiques et de communication électronique à des fins personnelles doit :

- Être raisonnable,
- Non lucrative,
- Ne pas nuire à la qualité du travail ni au bon fonctionnement des services,
- Ne pas être préjudiciable au système d'information.

En outre, en toutes circonstances, les Utilisateurs doivent adopter un comportement loyal, de bonne foi et s'engagent à protéger l'image du SPCPF.

À cet effet, les Utilisateurs doivent stocker leurs éventuels documents personnels et privés dans un répertoire labélisé à cet effet (« Personnel » ou « Privé »). De même, toute correspondance par la messagerie électronique qui serait personnelle doit être clairement identifiée comme telle en précisant le terme « Personnel » ou « Privé » dans le champ « Objet du message ».

En cas de présomption basée sur des indices d'une violation des dispositions de la présente charte ou d'une disposition légale ou réglementaire, des contrôles spécifiques portant sur l'utilisation des moyens informatiques et de communication électronique pourront être effectués.

III.2) Gestion des absences

Chaque Utilisateur doit veiller en cas d'absence temporaire à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service. En particulier, chaque Utilisateur doit veiller à mettre en place les mesures de gestion d'absence préconisées dans le livret technique en annexe de la présente charte informatique.

Pour les besoins de la continuité de l'activité, le département informatique peut être contraint d'accéder, dans le respect de la vie privée de l'Utilisateur, aux données stockées sur son poste de travail (fichiers, messageries, support de stockage). Dans ces conditions, l'accès aux données se fera dans le respect le plus strict des dispositions légales et notamment du droit au respect de la vie privée et le collaborateur concerné sera tenu informé des motifs de l'accès ainsi que des données recueillies.

Par ailleurs, en cas de **suspension du contrat de travail**, l'Utilisateur s'interdit d'utiliser les moyens informatiques et de communication électronique, les accès pouvant être désactivés pendant la durée de cette absence.

III.3) Gestion des départs

Lors de son départ du SPCPF, l'Utilisateur doit restituer au SPCPF, l'ensemble des moyens informatiques et de communication électronique, mis à sa disposition et ce en bon état de fonctionnement. En particulier, chaque Utilisateur doit veiller à mettre en place les mesures de gestion d'absence préconisées dans le livret technique en annexe de la présente charte informatique. Il appartient à l'Utilisateur de détruire son répertoire « Personnel » ou « Privé » lors de son départ.

Le répertoire « Personnel » ou « Privé » d'un Utilisateur quittant le SPCPF, s'il n'a pas été détruit par ce dernier au jour de son départ, est **supprimé sans copie** ni prise de connaissance préalable du contenu par le SPCPF.

Sauf nécessité liée à la continuité de service, le départ d'un Utilisateur entraîne la fermeture de sa boîte aux lettres électronique dans un délai défini par le livret technique en annexe de cette ce document. L'objectif est de rediriger les contacts de l'Utilisateur vers sa nouvelle boîte électronique ou vers les collaborateurs du SPCPF.

Il est de la responsabilité de l'Utilisateur de faire suivre ses messages à caractère privé en communiquant sa nouvelle adresse à ses interlocuteurs.

IV) LES REGLES GENERALES D'UTILISATION

IV.1) Dispositions générales

Les moyens informatiques, mis à disposition de l'Utilisateur, sont exclusivement installés, configurés et paramétrés par le personnel habilité du département informatique du SPCPF.

Tout Utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient entraîner des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom du SPCPF qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés ou reçus et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues, ainsi que des règles élémentaires de courtoisie et de bienséance.

IV.2) Les droits et les devoirs des Utilisateurs

La sécurité des moyens informatique et de communication électronique impose à chaque Utilisateur un engagement dans le respect de certaines règles.

IV.2.1) L'Utilisateur des ressources informatiques doit :

- Utiliser raisonnablement ces ressources ;
- Respecter l'intégrité et la confidentialité des données. Cette règle s'applique tant pour le traitement des informations que pour leur communication interne et externe.
- Respecter le droit de propriété intellectuelle : non-reproduction et/ou non-diffusion de données soumises à un droit de copie non détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Assurer la protection et notamment la confidentialité des données personnelles dans le respect du RGPD ;
- Respecter les règles relatives à la définition et au changement des mots de passe ;
- Respecter la gestion des accès, en particulier ne pas utiliser les identifiants et mots de passe d'un autre Utilisateur, ni chercher à connaître ces informations ;
- Signaler au département informatique du SPCPF toute possibilité technique d'accès à une ressource informatique qui ne correspond pas à son habilitation ; l'Utilisateur s'interdit toute divulgation de cette possibilité d'accès ;
- Limiter ses accès aux seules ressources pour lesquelles il est expressément habilité par son autorité hiérarchique ou par le DI, à l'exclusion de toute autre, même si cet accès est techniquement possible ;
- Assurer la protection des informations et plus particulièrement celles considérées comme sensibles. En particulier, il ne doit pas transporter, sans protection, des données sensibles sur des supports non fiables tels que des ordinateurs portables, des clés USB, des disques externes, etc ;
- Utiliser seulement le réseau WIFI « invité » pour connecter un équipement personnel en ayant un usage raisonnable de la connexion internet ;
- Respecter les contraintes liées à la maintenance du système d'information ;
- Avertir le département informatique du SPCPF de tous les dysfonctionnements techniques constatés et de toutes les anomalies découvertes, telles que les intrusions dans les systèmes d'information ;
- Sauvegarder régulièrement ses données ;
- Verrouiller sa session même en cas d'absence de courte durée ;
- Quitter les applications, éteindre son ordinateur et son écran (s'il existe) en fin de journée de travail ;

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

IV.2.1) L'Utilisateur des ressources informatiques NE doit PAS :

- Perturber la disponibilité du système d'information en ayant un usage excessif de la connexion internet partagée par tous les agents ou en utilisant l'espace de stockage réseau de façon non raisonnable et à des fins personnelles ;
- Transmettre des informations à caractère professionnel pour des fins personnelles par tout moyen (ex : par le biais d'une autre messagerie que celle mise à sa disposition par le SPCPF ; par le biais d'une clé USB ; etc.) ;
- Stocker ou transmettre des informations portant atteinte à la dignité humaine ;
- Ne pas inscrire dans les zones de libres commentaires des informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ni de données sensibles (ethnie, santé, religion, données d'infractions pénales et opinions politique, religieuse, syndicale, …) ;
- Masquer son identité ou usurper celle d'un autre ;
- Connecter des équipements personnels sur le réseau interne du SPCPF ;
- Installer, télécharger ou utiliser sur les moyens informatiques et de communication électronique un logiciel et/ou un progiciel sans autorisation du département informatique et sans qu'une licence d'utilisation appropriée n'ait été souscrite par le SPCPF ;
- Modifier ces équipements par l'ajout de logiciels et matériels n'appartenant pas au SPCPF ; dans le cas où ces logiciels et matériels lui sembleraient nécessaires pour l'exercice de sa mission, l'utilisateur en fait la demande au département informatique du SPCPF. À ce titre, la procédure est décrite dans le livret technique annexée à la présente charte informatique ;
- Réaliser des opérations de maintenance (logiciel et/ou matériel) si sa fonction ne l'y autorise pas ;
- Désactiver les programmes antivirus et pare-feu installés sur les moyens informatiques ;
- Ouvrir ou répondre à un mail suspect ;
- Chiffrer ses données professionnelles avec des moyens personnels qui ne permettent pas au SPCPF de les déchiffrer.

En cas d'utilisation inappropriée, le SPCPF peut interrompre, modifier ou supprimer à tout Utilisateur l'accès à tout ou partie des moyens informatiques et de communication électronique de manière temporaire ou définitive.

IV.3) Les droits et les devoirs du SPCPF

Le SPCPF doit veiller à la disponibilité et à l'intégrité du système d'information.

En ce sens, il s'engage à :

- Mettre à disposition les **ressources informatiques** matérielles et logicielles nécessaires au bon déroulement de la mission des Utilisateurs.
- Mettre en place des **programmes de formations** adaptés et nécessaires aux Utilisateurs pour une bonne utilisation des outils.
- Informer les Utilisateurs des diverses **contraintes d'exploitation** (interruption de service, maintenance, modification de ressources, …) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les **mises à jour** nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la **confidentialité des "données Utilisateurs"** auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.
- Définir les **règles d'usage** de son système d'information et veiller à leur application.

IV.4) Confidentialité et intégrité des données

Chaque Utilisateur doit assurer la confidentialité et l'intégrité des données qu'il est amené à traiter dans le cadre de ses activités.

V) LES ACCES

Chaque Utilisateur, le jour de sa prise de fonction au SPCPF, reçoit un droit d'accès individuel matérialisé par tout moyen physique ou logique (exemple : identifiant et mot de passe ou badge ou carte ou clé). L'accès aux moyens informatiques et de communication électronique nécessite une autorisation préalable et passe par l'affectation d'un compte avec un identifiant et un mot de passe.

Ce droit d'accès peut être différent d'un Utilisateur à l'autre selon le profil de chacun, lequel est attribué en considération de la mission, de la nature du poste et des besoins professionnels.

Dans la mesure du possible, les identifiants et mots de passe ne doivent être conservés sous quelques formes que ce soit. Ceux-ci ne doivent en aucun cas, être enregistrés sur les navigateurs du poste de travail de l'Utilisateur. L'Utilisateur devra prendre les mesures nécessaires liées au niveau de sécurité et de gestion de ses accès présentés dans le livret technique en annexe de la présente charte informatique.

L'Utilisateur est responsable de l'utilisation qui est faite de son droit d'accès : sauf à avoir engagé préalablement une demande de suppression ou de suspension de son droit d'accès, ou à en rapporter la preuve contraire, toute utilisation des moyens informatiques et de communication électronique est réputée avoir été réalisée par le porteur de l'identifiant d'accès qui en assume les conséquences juridiques et financières.

En cas d'utilisation inappropriée, le SPCPF peut interrompre, modifier ou supprimer à tout Utilisateur l'accès à tout ou partie des moyens informatiques et de communication électronique de manière temporaire ou définitive.

VI) LES EQUIPEMENTS INFORMATIQUES

Le présent chapitre a pour objectif d'établir les règles de gestion et d'utilisation des équipements informatique d'attribution, de prêt et nomades. Il règlemente également l'utilisation d'équipements personnels à des fins professionnelles.

L'Utilisateur est responsable des équipements informatiques mis à sa disposition. Il est tenu d'utiliser le matériel informatique qui lui est confié de manière prudente et attentive. Il devra à ce titre mettre en place les mesures nécessaires à la protection de ce matériel, définies par le livret technique et annexé à la présente charte informatique.

VII) LA MESSAGERIE ELECTRONIQUE

VII.1) Principes généraux

Chaque Utilisateur, dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique. Elle est de la forme suivante : prénom.nom@spc.pf. Il est tenu de la consulter au minimum une fois par jour, hormis en période d'absence.

L'attention des Utilisateurs est attirée sur le fait qu'une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (ordonnance 2005-1516 du 8 décembre 2005). Ils doivent en conséquence être traités dans les mêmes délais. Il convient donc de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale du SPCPF et/ou de l'Utilisateur.

L'Utilisateur doit veiller au respect des lois et règlements, notamment à la protection des droits intellectuelle et des droits des tiers. L'Utilisateur devra soigner la qualité des informations envoyées à l'extérieur et s'engage, donc, à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine, à la vie privée, aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

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

VII.2) Envoi de messages électroniques

Avant tout envoi, il est impératif que l'Utilisateur vérifie la liste de destinataires du message et de leur qualité à recevoir une communication des informations transmises. En présence d'informations confidentielles et/ou de données personnelles et/ou sensibles, ces vérifications doivent être renforcées.

Dans le cas échéant, l'Utilisateur doit respecter les circuits de l'organisation ou la voie hiérarchique.

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

L'Utilisateur signe tout courriel professionnel. La signature d'un courrier électronique fait l'objet d'une forme standardisée et comporte obligatoirement :

- Le nom et prénom de l'expéditeur ;
- Son entité de rattachement ;
- Les coordonnées postales du SPCPF.

Les Utilisateurs s'engagent à respecter ce format en évitant tout élément complémentaire.

VII.3) Réception de messages électroniques

L'Utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect. À ce titre, l'utilisateur devra mettre en place les mesures définis par le livret technique en annexe de cette charte informatique.

VII.4) Absence de l'Utilisateur

L'Utilisateur est informé qu'en cas d'absence prolongée, de suspension de contrat et pour la continuité des services, le département informatique se réserve le droit d'accéder à sa messagerie et à ses dossiers professionnels, et ce, sans consentement préalable et dans le respect des lois et règlements.

L'Utilisateur doit activer la fonction de notification d'absence afin de prévenir toute discontinuité dans le traitement des messages et de permettre à ses correspondants de prendre les mesures appropriées.

VII.5) Utilisation personnelle

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins, il est **toléré**, en dehors des heures de travail, un usage modéré de celle-ci pour des besoins personnels et ponctuels. Tout message électronique à caractère personnel émis ou reçu doit comporter, dans son objet, la mention « Personnel » ou « Privé ». Ces derniers ne pourront alors être ouverts par la Direction générale ou le département informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la loi. Tout message ne comportant pas cette mention est présumé être un message professionnel, susceptible d'être consulté par tout Utilisateur habilité à le faire et par l'autorité hiérarchique.

La lecture des courriels personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle.

Toutefois, les Utilisateurs sont invités à utiliser, dans la mesure du possible, leur messagerie personnelle pour l'envoi de message à caractère personnel plutôt que la messagerie professionnelle.

VIII) LA TELEPHONIE

VIII.1) Principes généraux

Chaque Utilisateur, dans le cadre de son activité professionnelle peut disposer, selon son profil, et sous réserve d'autorisation de sa hiérarchie, de moyens de télécommunication consistant en des équipements terminaux de télécommunication (poste téléphonique fixe et/ou poste téléphonique mobile, appareil de visio-conférence, d'un smartphone, d'une tablette ou d'une clé 3G, 4G ou plus, ou hot spot wifi).

Concernant l'utilisation des terminaux ayant accès à des sites internet ou à la messagerie électronique, les règles édictées dans la présente charte s'appliquent également.

L'Utilisateur est informé qu'un journal des communications, entrantes et/ou sortantes de la téléphonie fixe et mobile, est accessible par les administrateurs réseau du département informatique. Il est aussi informé que les relevés de communication peuvent faire l'objet d'un contrôle.

VIII.2) Engagement de l'Utilisateur vis-à-vis de la téléphonie mobile

L'Utilisateur s'engage à :

- Prévenir le département informatique sans délai en cas de perte, vol ou de faille de sécurité.
- Mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone et qui sont demandés et principalement le code d'accès.
- Utiliser des codes d'accès (pins, verrouillage clavier, etc…)
- Se déconnecter de toutes les applications après usage et ne pas rester connecté par défaut
- Être vigilants vis-à-vis des données contenues dans le smartphone.

L'Utilisateur est attiré sur le fait qu'un SMS ou l'utilisation de messages instantanés tels que le « chat » n'a pas la même portée qu'un courrier manuscrit ou électronique.

VIII.3) Utilisation personnelle du téléphone

Au même titre que la messagerie électronique, l'utilisation personnelle du téléphone fixe ou mobile est tolérée, à condition qu'elle reste dans des limites raisonnables tant en termes de temps passé que de quantité d'appels.

IX) USAGE DE L'INTERNET

IX.1) Principes généraux

Dans le cadre de leur activité, un accès à Internet est mis à disposition de l'Utilisateur. Cependant, l'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

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

L'Utilisateur est informé que pour des raisons de sécurité ou de déontologie, l'accès à certains sites est rendu impossible par la direction du SPCPF. Il s'interdit donc de contourner les mesures techniques de blocage et de filtrage mises en œuvre par le département informatique du SPCPF.

Il est rappelé que les Utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts du SPCPF, y compris sur Internet.

IX.2) Le Wifi interne et Wifi externe

L'Utilisateur est informé qu'un réseau Wifi interne (réservé uniquement aux agents du SPCPF) et un réseau Wifi externe (réservé aux élus, prestataires, invités ou tiers extérieurs au SPCPF, ou autre souhaitant accéder à un réseau internet), sont disponibles au sein du SPCPF. L'Utilisateur devra prendre connaissance de la procédure d'utilisation de ces deux réseaux Wifi.

IX.3) Consultation

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

Toute saisie d'informations impactant des données sensibles professionnelles sur un site Internet professionnel nécessite l'autorisation préalable de la Direction générale.

IX.1) Plate-forme collaborative - Forums

La participation à des listes de diffusion, forums de discussions et de discussion en ligne est susceptible d'engager la responsabilité de l'auteur de la contribution.

L'Utilisateur doit s'abstenir de porter atteinte à l'image ou aux intérêts du SPCPF ou de ses clients, ou aux droits de tiers. Il doit être particulièrement vigilant à l'égard de la nature des informations qu'il communique et s'en référer à son supérieur hiérarchique en cas de doute.

IX.2) Téléchargement

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

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

Pour éviter les abus, la Direction générale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

IX.3) La messagerie instantanée

Il est interdit à l'Utilisateur d'utiliser d'autres systèmes de messagerie instantanée que ceux mis à sa disposition.

X) IMPRESSION

Les impressions sont présumées professionnelles mais une utilisation personnelle raisonnable est tolérée.

Sobriété numérique : l'Utilisateur doit veiller à réduire au maximum ses impressions. Si l'impression est indispensable, il faut également veiller à imprimer les feuilles en recto-verso et si possible en noir et blanc afin de limiter les coûts. Pour rappel, une impression couleur vaut plus cher qu'une impression en noir et blanc.

XI) LES SAUVEGARDES

Les Utilisateurs sont informés que le département informatique du SPCPF réalise des sauvegardes périodiques de toutes les données sur le réseau, qui ont un caractère professionnel.

Les sauvegardes sont réalisées sur les fichiers du serveur et les logiciels fournis officiellement par le SPCPF. Ne sont pas sauvegardées, les données des Utilisateurs, taguées comme « Privée » ou « Personnel » et les données stockées localement sur l'équipement de l'Utilisateur.

Il convient à chacun de privilégier l'enregistrement des données professionnelles sur le serveur.

XII) LES MISES A JOUR

Des mises à jour sont paramétrées sur l'ensemble des outils officiellement fournis par le SPCPF. Elles sont indispensables car elles permettent de corriger les failles de sécurité des logiciels.

Les mises à jour ne sont pas toutes automatisées. Ainsi il conviendra à chacun de réaliser ces mises à jour lorsque vous êtes invités à le faire. Des consignes particulières pourront être données par le département informatique.

Appliquez une grande vigilance quant à l'origine de ces demandes.

XIII) TELECHARGEMENT ET INSTALLATION DE LOGICIEL

Tous les téléchargements, installations de logiciel sur le poste informatique professionnel de l'utilisateur doit recueillir l'aval du département informatique. Il est interdit de copier ou installer des fichiers susceptibles de créer un risque de sécurité pour le SPCPF.

Dans tous les cas, ces logiciels doivent respecter la règlementation en vigueur, et les mesures de sécurité fondamentales. Les téléchargements doivent provenir des sites officiels.

XIV) LE TELETRAVAIL

La présente partie concerne l'utilisation des systèmes d'information du SPCPF, de ses ressources, et des moyens de communication par l'Utilisateur lorsque celui-ci est situé en dehors du site physique du SPCPF.

En premier lieu, il convient de préciser que l'ensemble des dispositions de la présente charte sont applicables aux Utilisateurs accédant aux systèmes d'information et de communication du SPCPF à distance. À ce titre, l'Utilisateur mettra en place les mesures de sécurité préconisées dans le livret technique en annexe de la présente charte informatique.

XV) MESURES DE CONTROLE

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable du département informatique et de la Direction générale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés et du RGPD.

XV.1) Surveillance

Les moyens informatiques et de communication électronique peuvent donner lieu à une surveillance et un contrôle à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Dans le cadre des opérations de contrôle effectuées par le SPCPF, l'Utilisateur est informé que les administrateurs système et de réseaux peuvent notamment être amenés à ouvrir tout message ou fichier figurant sur la messagerie, et à vérifier l'ensemble des connexions dudit Utilisateur.

Lors de ces accès, ces personnes sont tenues de respecter la confidentialité des informations, auxquelles elles accèdent, vis-à-vis des tiers à la mission de surveillance et de contrôle.

L'usage des services Internet peut faire l'objet d'un contrôle a posteriori. Ce contrôle peut porter sur le temps de connexion par poste ou sur les sites les plus consultés. Le département informatique du SPCPF a ainsi mis en place un système permettant d'assurer la traçabilité des accès internet et/ou des données échangées et se réserve le droit de procéder au filtrage des sites. Les traces correspondantes aux connexions et aux sites internet accédés par l'Utilisateur sont conservées pendant une durée d'un an.

Le SPCPF s'engage à réaliser les contrôles qu'il estime indispensables à la sauvegarde de ses intérêts, dans le respect strict des dispositions légales et réglementaires en vigueur.

XV.2) Messagerie électronique

À titre d'illustration, les contrôles automatiques relatifs à la messagerie peuvent porter sur :

- Le nombre de messages émis ou reçus vers l'extérieur,
- Le volume occupé par l'ensemble des boites aux lettres sur les serveurs de messagerie,
- La nature ou le format des pièces jointes.

Il peut en résulter :

- La mise en place de quota aux tailles des boites aux lettres,
- La suppression automatique de pièces jointes si un risque d'infection virale est détecté,
- La suppression automatique des messages de type non sollicités (spam).

XV.3) Gestion des répertoires

À titre d'illustration, les contrôles automatiques relatifs aux répertoires peuvent porter sur :

- Le volume occupé par l'ensemble des fichiers sur les serveurs,
- La nature ou le format des fichiers.

Il peut en résulter :

- La mise en place de quota sur les répertoires des serveurs de fichiers.

Par ailleurs, chaque Utilisateur est informé que les fichiers illicites pourront être automatiquement supprimés des serveurs (quel que soit le répertoire de stockage).

XV.4) Maintenance

La mise à disposition de moyens informatiques et de communication électronique implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

Ces opérations de maintenance peuvent nécessiter l'intervention d'une « personne habilitée » sur site ou sous la forme d'une « prise de main à distance ». La « personne habilitée » est la personne désignée à cet effet par le département informatique du SPCPF.

L'objectif de ces opérations est d'assurer le bon fonctionnement et la sécurité des systèmes d'information. Cependant, dans le cadre de ces interventions, la « personne habilitée » peut être amenée à prendre connaissance de messages émis ou reçus par l'Utilisateur et à examiner en détail le journal de ses connexions.

La « personne habilitée » fera en sorte de ne pas accéder à tout élément identifié comme « Personnel » ou « Privé » en dehors de la présence de l'Utilisateur. Cependant, elle peut y être contrainte pour des raisons de sécurité ou pour des raisons techniques (surcharge du système, lutte antivirus, lutte antispam, etc.) et ce, malgré l'opposition de l'Utilisateur.

Nota : la « prise en main à distance » déclenche au préalable un message d'information et nécessite l'accord formel de l'Utilisateur.

XV.5) Confidentialité des administrateurs système et réseau

Les administrateurs des systèmes informatiques qui ont pour mission de garantir la qualité de service et la pérennité du système informatique sont soumis aux dispositions de la « charte administrateur », ils sont notamment tenus de respecter les règles déontologiques suivantes : confidentialité des données et utilisation de leurs droits d'administrateurs à des fins strictement professionnelles.

XVI) RESPONSABILITE ET SANCTION

La loi, les textes réglementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout Utilisateur du système d'information du SPCPF n'ayant pas respecté la loi pourra être poursuivi pénalement.

En outre, tout Utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à l'établissement et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par la Direction générale.

XVII) RESPECT DES LOIS ET REGLEMENTATION

XVII.1) Le règlement général sur la protection des données (RGPD)

L'Utilisateur est informé de la nécessité de respecter les dispositions légales en matière de « traitement de données personnelles », conformément au **règlement n°2016/679 du 27 avril 2016**, dit règlement général sur la protection des données (RGPD) et à **l'ordonnance n°2018-1125 du 12 décembre 2018** prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

L'Utilisateur est également informé que lors de l'utilisation des outils et du matériel informatique mis à disposition par le SPCPF, ce dernier traite ses données pour assurer la sécurité de son système d'information. Le SPCPF est responsable du traitement des données à caractère personnel qui sont collectées. Pour plus d'informations concernant ce traitement de données à caractère personnel, l'Utilisateur peut consulter la politique de protection des données disponible sur le site internet spc.pf. Conformément à la législation Informatique et Libertés, l'Utilisateur dispose des droits suivants sur ses données dans les conditions qu'elle prévoit : droit d'accès, droit de rectification, droit à l'effacement (droit à l'oubli), droit d'opposition, droit à la portabilité et droit à la limitation du traitement. L'Utilisateur a également le droit de définir des directives relatives à la conservation, à l'effacement et à la communication de vos données après votre décès. Vous pouvez exercer ces droits auprès du Délégué à la protection des Données dont les coordonnées sont disponibles dans le livret technique annexé à la présente charte informatique. Sous réserve d'un manquement aux dispositions ci-dessus, il a le droit d'introduire une réclamation auprès de la CNIL (www.cnil.fr).

La notion de « données personnelles » correspond à toutes les informations se rapportant à une personne physique identifiée ou identifiable. L'identification d'une personne physique peut être réalisée :

- **Directement** (exemple : nom, prénom)
- **Indirectement** (exemple : n° client, numéro de téléphone, une donnée biométrique, plusieurs éléments propres à son identité physique, physiologique, génétique, etc…)
- **A partir d'une seule donnée** (exemple : ADN, n°CPS, etc…)

- **A partir du croisement d'un ensemble de données** (exemple : femme vivant à telle adresse, née tel jour, militant dans une association de jeunesse etc…)

Le traitement de données personnelles n'est pas obligatoirement informatisé, les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Tout traitement de données doit avoir un objectif, une finalité qui doit, bien évidemment, être conforme au RGPD, légal et légitime au regard de l'activité professionnelle du SPCPF.

En conséquence, tout Utilisateur souhaitant procéder à ce genre de traitement devra en informer préalablement le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le département informatique du SPCPF qui prendra les mesures nécessaires au respect des dispositions légales.

XVII.2) Autres dispositions

Dans le cadre de son activité, le SPCPF est soumis à diverses règlementations spécifiques, afin de s'assurer que l'utilisation des données par chaque Utilisateur se fait en conformité avec la règlementation. Les Utilisateurs s'engagent à utiliser, manipuler et communiquer les données du SI dans le strict respect de ces conditions.

L'Utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par l'ordonnance n° 2005-10 du 4 janvier 2005.

XVII.2.1) Les textes législatifs

- **Loi du 06/01/1978** relative à l'informatique, aux fichiers et aux libertés.

  Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

- **Loi du 17/07/1978** portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

- **Loi du 03/07/1985** relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.

  Elle interdit à l'Utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

- **Loi du 05/01/1988** sur la fraude informatique.

  Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :

  - Les accès ou maintien frauduleux dans un système d'information
  - Les atteintes accidentelles ou volontaires au fonctionnement
  - La falsification des documents informatiques et leur usage illicite
  - L'association ou l'entente en vue de commettre un de ces délits

- **Loi du 10/07/1991** relative au secret des correspondances émises par voie des télécommunications.

- **Loi du 13/03/2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

- **Loi du 14/03/2011** (dite LOPPSI) d'orientation et de programmation pour la performance de la sécurité intérieure.

- **Loi du 30/10/2017** renforçant la sécurité intérieure et la lutte contre le terrorisme

XVII.2.2) Le droit disciplinaire

- **Ordonnance n°2005-10 du 4 janvier 2005** portant statut général des fonctionnaires des communes et des groupements de communes de la Polynésie française ainsi que de leurs établissements publics administratifs.

- **Décret n° 2011-1040 du 29 août 2011** fixant les règles communes applicables aux fonctionnaires des communes et des groupements de communes de la Polynésie française ainsi que de leurs établissements publics administratifs.

- **Décret n° 2011-1551 du 15 novembre 2011** portant diverses dispositions relatives à la fonction publique des communes et des groupements de communes de la Polynésie française ainsi que de leurs établissements publics administratifs.

- **Décret n° 2011-1552 du 15 novembre 2011** portant dispositions applicables aux agents non titulaires des communes et des groupements de communes de la Polynésie française ainsi que de leurs établissements publics administratifs.

XVII.2.3) Le code pénal

- **Article 323-1** : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

- **Article 323-2** : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

- **Article 323-3** : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

- **Article 323-3-1** : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- **Article 323-4** : La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- **Article 323-5** : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

- **Article 323-6** : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

- **Article 323-7** : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Corruption : La corruption se définit comme l'agissement par lequel une personne investie d'une fonction déterminée, publique ou privée, sollicite/propose ou agrée/cède, un don, une offre ou une promesse, en vue d'accomplir, retarder ou omettre d'accomplir un acte entrant, d'une façon directe ou indirecte, dans le cadre de ses fonctions. Le délit de corruption est prévu aux articles 433-1 et 433-2 du code pénal. Exemples :

- Le **trafic d'influence** se définit comme « le fait, par une personne dépositaire de l'autorité publique, chargée d'une mission de service public, ou investie d'un mandat électif public, de solliciter ou d'agréer, sans droit, à tout moment, directement ou indirectement, des offres, des promesses, des dons, des présents ou des avantages quelconques pour elle-même ou pour autrui : soit pour accomplir ou s'abstenir d'accomplir un acte de sa fonction, de sa mission ou de son mandat ou facilité par sa fonction, sa mission ou son mandat ; soit pour abuser de son influence réelle ou supposée en vue de faire obtenir d'une autorité

ou d'une administration publique des distinctions, des emplois, des marchés ou toute autre décision favorable. »
Le délit de trafic d'influence est prévu par l'article 432-11 du code pénal.

- La **concussion** se définit comme le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, de recevoir, exiger ou ordonner de percevoir à titre de droits ou contributions, impôts ou taxes publics, une somme qu'elle sait ne pas être due, ou excéder ce qui est dû.
  Le délit de concussion est prévu par l'article 432-10 du code pénal.
- La **prise illégale d'intérêt** se définit comme le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ou par une personne investie d'un mandat électif public, de prendre, recevoir ou conserver, directement ou indirectement, un intérêt quelconque dans une entreprise ou dans une opération dont elle a, au moment de l'acte, en tout ou partie, la charge d'assurer la surveillance, l'administration, la liquidation ou le paiement.
  Le délit de prise illégale d'intérêt est prévu par l'article 432-12 et l'article 432-13 du code pénal.
- Le **favoritisme** se définit comme le fait par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ou investie d'un mandat électif public ou exerçant les fonctions de représentant, administrateur ou agent de l'Etat, des collectivités territoriales, des établissements publics, des sociétés d'économie mixte d'intérêt national chargées d'une mission de service public et des sociétés d'économie mixte locales ou par toute personne agissant pour le compte de l'une de celles susmentionnées de procurer ou de tenter de procurer à autrui un avantage injustifié par un acte contraire aux dispositions législatives ou réglementaires ayant pour objet de garantir la liberté d'accès et l'égalité des candidats dans les marchés publics et les délégations de service public.
  Le délit de favoritisme est prévu par l'article 432-14 du code pénal.

XVIII) CHAMP LEXICAL

SYSTEME D'INFORMATION :

Ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation (du SPCPF).

RESSOURCES INFORMATIQUES :

- le matériel
- les logiciels et les procédures
- les données et les fichiers

INTERNET :

Interconnexion mondiale de réseaux reposant sur un protocole appelé « Internet » et dont les applications les plus utilisées sont le courriel et les consultations de sites (Web).

INTRANET :

Utilisation des technologies liées à Internet au sein d'un réseau local. Les principaux intérêts sont de faciliter et de rendre plus conviviale l'accès aux données par l'utilisation du navigateur et de la messagerie interne.

EXTRANET :

On peut dire que c'est un « Intranet » étendu à des Utilisateurs extérieurs qui, n'étant pas situés sur le réseau local, seront soumis à un accès sécurisé.

COURRIEL : message électronique ou E-mail

RESEAU :

Ensemble d'ordinateurs et de machines informatiques qui communiquent grâce à une technique commune de transmission.

PERIPHERIQUES :

Matériels connectés à un poste de travail ou directement sur le réseau local (exemples : imprimante, scanners…)

ADMINISTRATEUR SYSTÈME ET RESEAU :
Membre du département informatique en charge des ressources informatiques. Il est soumis au secret professionnel en ce qui concerne les données personnelles ou confidentielles dont il pourrait être amené à prendre connaissance dans l'exercice de ses fonctions.