PRÉFET
ADMINISTRATEUR SUPÉRIEUR
DES TERRES AUSTRALES
ET ANTARCTIQUES
FRANÇAISES
Liberté
Égalité
Fraternité

Direction des Services Techniques
Service de l'Informatique,
des Télécommunications et des Réseaux

Affaire suivie par :
Fabrice MONTFORT, Cyril RAISON
STIR
Tél : 02 62 96 78 60 / 02 62 96 78 36
Mél : fabrice.montfort@taaf.fr / cyril.raison@taaf.fr

Réf : TAAF/STIR-CITD2021

Saint-Pierre, le 30/07/2021

CHARTE D'UTILISATION DES SERVICES ET RESSOURCES INFORMATIQUES ET DE COMMUNICATION

1. Présentation du réseau informatique et téléphonique

Les Terres australes et antarctiques françaises - TAAF (service des télécommunications, de l'informatique et des réseaux - STIR) mettent à disposition des utilisateurs dans les districts et sur le Marion Dufresne un certain nombre de postes de travail informatiques raccordés à un réseau donnant accès à internet via une liaison VSAT.

Ce réseau informatique est placé sous la responsabilité opérationnelle des Acteurs de la Sécurité des Systèmes d'Information (ASSI) des TAAF. Ces ASSI peuvent être amenés à surveiller ce réseau. Ils rendent compte régulièrement à leurs autorités hiérarchiques au sein des TAAF et du Ministère de l'Intérieur. Ils sont en poste au siège des TAAF à Saint-Pierre et assurent la coordination avec les Bureaux Communication Radio (BCR) des districts, garants de la bonne application de la présente charte.

Un certain nombre de règles d'utilisation du réseau informatique est à prendre en compte pour tout utilisateur qui aurait à accéder aux serveurs locaux ou à internet depuis un poste de travail informatique directement ou indirectement relié à ce réseau.

Ces règles sont distinctes de celles de l'internet sécurisé par ORION – accessible via le RIE (Réseau Interministériel d'Etat) – lesquelles font l'objet d'un document spécifique nommé « Charte ORION » qui ne s'applique pas à l'heure actuelle dans les districts des TAAF.

Par ailleurs, le STIR met à disposition des utilisateurs, dans les districts et sur le Marion Dufresne, un certain nombre de postes téléphoniques raccordés à cette même liaison VSAT.

Ce réseau téléphonique est régi par des règles spécifiques qui sont à prendre en compte pour toute utilisation d'un poste téléphonique directement ou indirectement relié à ce réseau.

Le STIR met en outre à disposition des utilisateurs dans les districts des radios UHF/VHF pour assurer la sécurité sur base et organiser les opérations lors des rotations. L'utilisation de ces radios nécessitent la prise en compte de quelques règles d'usages pour permettre un trafic propre sur les bons canaux et en respectant certaines conventions.

Enfin, en cas de défaillance grave des systèmes VSAT, le STIR met à disposition dans chaque district des moyens satellitaires de secours (FBB et Iridium). Ces moyens de secours sont réservés aux urgences et sont disponibles à l'hôpital, au BCR et au bureau du Chef de District.

2. Objet du document

L'utilisation de tout Système d'Information (SI) relié à un réseau informatique suppose, de la part des utilisateurs et des administrateurs, le respect de certaines règles dont le rôle est d'assurer :

- La disponibilité du Système d'Information :
  Capacité du système à assurer une continuité de fonctionnement permettant à l'ensemble des utilisateurs de pouvoir utiliser le système et à accéder aux ressources nécessaires à la demande.

- L'intégrité du Système d'Information :
  Capacité du système à assurer la justesse des informations gérées et à éviter toute altération ou destruction par accident ou malveillance.

- La confidentialité du Système d'Information :
  Capacité du système à limiter l'accès aux informations aux seules personnes habilitées.

En d'autres termes, il est impératif de disposer d'un Système d'Information fournissant la bonne information (intégrité) à la bonne personne (confidentialité) au bon moment (disponibilité).

Cette charte a pour but de faciliter l'apprentissage et l'utilisation optimale de l'outil informatique et d'informer les utilisateurs quant aux procédures mises en œuvre au sein des Terres Australes et Antarctiques Françaises pour y parvenir. Elle est applicable à tous les utilisateurs et aux administrateurs des réseaux informatiques, présents dans les districts et sur le Marion Dufresne, qui s'engagent à la respecter.

Elle décrit en outre, aussi précisément que possible, les modalités d'utilisation des outils de communication tels que la téléphonie ou les radios HF mises à disposition dans les districts et sur le Marion Dufresne des TAAF.

Elle est basée sur l'application de textes réglementaires. Elle énumère les droits et devoirs des utilisateurs et des administrateurs du système. Elle est révisable en fonction de l'évolution des solutions techniques et du réseau, la dernière version étant diffusée aux Chefs de district, Chefs de mission et aux BCR de chaque district.

3. L'informatique

A. La sécurité

Les moyens mis en œuvre par les TAAF correspondent à un niveau élevé de sécurité.

Les serveurs sont contrôlés par un anti-virus dédié, mis à jour quotidiennement. Les courriels sont filtrés par un anti-virus sur le serveur de messagerie et chaque ordinateur présent sur le réseau est équipé d'un anti-virus installé localement. Tous sont mis à jour quotidiennement.

Le transfert de fichiers par courriel avec des extensions sensibles (fichiers exécutables) est interdit et bloqué (fichiers avec extension du type *.exe, *.com, *.bat, …).

La sécurité du réseau est assurée par un pare-feu de dernière génération dont les règles sont gérées par le BCR sous la responsabilité du STIR.

Les systèmes d'exploitation sont mis à jour automatiquement par la solution Microsoft WSUS (l'équivalent de Microsoft Update sur Internet). Ces mises à jour permettent de contrer les failles de sécurité des systèmes Microsoft Windows.

La navigation sur internet est limitée par une solution de filtrage d'URL automatique (PFSENSE) qui interdit l'accès aux sites sensibles (listes blanches et listes noires fournies par le Ministère de l'Intérieur) pour les postes en libre accès et qui n'autorise l'accès qu'à des sites spécifiques (cf. liste des sites autorisés par le siège en Annexe 1).

Le mot de passe de chaque utilisateur est personnel et confidentiel. Il ne doit en aucun cas être connu des administrateurs du réseau ni des Acteurs de la Sécurité des Systèmes d'Information du siège. Chaque utilisateur peut, à sa guise et quand il le désire, changer son mot de passe. Pour des raisons de sécurité, les ASSI se réservent le droit de forcer le changement de mot de passe, voire d'automatiser ce changement à une fréquence raisonnable qui sera précisée. Il est interdit de communiquer son mot de passe à autrui. En cas de doute, l'utilisateur doit immédiatement contacter le BCR – qui remontera l'information au STIR – et changer son mot de passe.

Règles en vigueur

Le mot de passe est la clé de sécurité d'accès. Ce système d'authentification n'est efficace que si chacun respecte le caractère confidentiel de son mot de passe.

Ne le confiez à personne. Si un(e) collègue doit accéder à vos dossiers en votre absence, consultez le BCR.

N'affichez jamais votre mot de passe. Le mot de passe prendra la forme d'une chaîne de caractères alphanumériques composée de 5 caractères alphabétiques et de 3 caractères numériques a minima.

Les utilisateurs ne doivent en aucun cas tenter de contourner ces solutions de protection ou d'empêcher leur bon fonctionnement, notamment en désactivant l'anti-virus local. Ils s'engagent à respecter la loi en termes d'utilisation des moyens mis à disposition par les TAAF.

La manière préventive la plus efficace de lutte antivirale est de se méfier de toute source de données venant de l'extérieur (fichiers transmis par courriel, navigation internet, clés USB et autres supports amovibles, …). Pour ce faire, et en l'absence de station blanche, l'utilisateur devra systématiquement scruter ces informations à l'aide de l'anti-virus. En cas de doute sur l'expéditeur d'un courriel ou de sa pièce jointe, il convient de supprimer le mail et de ne pas ouvrir la pièce jointe.

Une solution automatique de mise en quarantaine a été mise en œuvre, les logiciels anti-virus installés tant au niveau des serveurs que des postes de travail émettent des alertes en cas de détection virale. Si ces alertes deviennent systématiques, il convient de prévenir le BCR qui procédera à la mise en quarantaine de la station informatique. Le poste de travail sera déconnecté du réseau et le compte utilisateur suspendu jusqu'à ce que l'origine de l'attaque soit établie et solutionnée. La station de travail et le compte utilisateur ne seront réintégrés au réseau qu'après validation par le BCR et le STIR des actions correctives menées.

Une autre faille de sécurité est l'accès aux postes de travail ou aux données stockées en local. Il existe quelques solutions simples qui permettent de garantir un minimum de sécurité d'accès à ces informations.

Lorsque l'utilisateur quitte son poste, même momentanément, il doit systématiquement fermer sa session ou mettre son poste de travail en veille. Cette manipulation évite toute intrusion intempestive sur une station dont la session est déjà ouverte, sans avoir besoin de taper un mot de passe. Le STIR se réserve le droit de demander aux différents BCR de paramétrer l'option de mise en veille par défaut, et il sera interdit de la désactiver.

Seuls les BCR, sous la responsabilité du STIR, sont habilités à paramétrer les postes de travail. Des moyens sont mis en œuvre afin de s'assurer qu'aucun logiciel ne soit installé sans licence régulière et valide. Le BCR peut, sans préavis, supprimer toute application ou logiciel « pirate » d'un poste de travail.

Bien que ces moyens correspondent à un niveau de sécurité élevé, aucune solution n'est fiable à 100%. Le STIR décline toute responsabilité quant à d'éventuelles pertes d'informations ou destructions liées à une éventuelle attaque virale ou de piratage. Le STIR assurera, via le BCR, la mise à niveau des équipements touchés, dans les délais les plus courts, en tenant compte de l'ampleur des dégâts causés par l'attaque.

Les choix liés à la sécurité (stratégies, outils et services) sont du ressort exclusif du siège des TAAF.

En cas d'urgence, le STIR se réserve le droit d'isoler tout ou partie du réseau, des postes de travail, des serveurs et éléments actifs du réseau ou de déconnecter des utilisateurs pour éviter une infection virale généralisée.

B. Messagerie électronique

Chaque utilisateur peut disposer d'une adresse de messagerie électronique personnalisée sur simple demande. Pour des raisons d'homogénéité et de lisibilité, l'adresse courriel prend la forme « prénom.nom@ams-taaf.fr », « prénom.nom@ker-taaf.fr », « prénom.nom@cro-taaf.fr » ou « prénom.nom@ta-taaf.fr » selon le district dans lequel est basé l'utilisateur. Des exceptions liées à la longueur de noms composés peuvent être accordées par le STIR.

Le STIR met à disposition des utilisateurs ayant des besoins spécifiques en matière de confidentialité et d'échange de données sensibles des comptes de messagerie sécurisée Nomade 2.0. L'accès à ce service se fera via un webmail du Ministère de l'Intérieur et une charte spécifique (Charte Nomade) devra être signée par l'agent concerné. Seul le STIR dispose de la compétence pour créer une adresse Nomade 2.0 et elle mandatera le BCR pour l'installation et le paramétrage des certificats de sécurité. L'utilisateur recevra directement son mot de passe, sans intermédiaire.

La messagerie électronique est un précieux outil de communication. Même si elle est personnelle et confidentielle pour chaque utilisateur, elle doit être considérée comme un outil de travail et non comme un outil personnel.

Chaque utilisateur est responsable de l'utilisation de sa boîte aux lettres (BAL) et doit respecter certaines règles.

Sont interdits :

- Les messages à caractère politique, raciste, pornographique et les insultes ;
- Les messages à caractère syndical, autres que des convocations aux réunions des différentes instances légales ;
- Les messages généraux (diffusion à l'ensemble des personnels sur bases) traitant d'activités extra-professionnelles (telles que des vœux, petites annonces, chaînes de solidarité, ventes quelconques, invitations, concerts, …) ;
- L'ouverture de pièces jointes reçues de correspondants inconnus, surtout celles comportant des extensions sensibles (*.exe, *.com, *.bat, …) ;
- Le masquage de l'identité par quelque procédé que ce soit ;
- L'envoi de données confidentielles ou nominatives à l'extérieur de la collectivité des TAAF.

Plus généralement, les règles d'éthique professionnelle, de secret professionnel, d'obligation de réserve sont applicables.

La boîte aux lettres est stockée soit localement sur le poste de travail, soit sur le serveur de messagerie, chacune des deux solutions ayant ses avantages et inconvénients. Si la boîte aux lettres est stockée localement sur le poste de travail (disque dur), les mails déjà reçus ou émis sont accessibles sans connexion au serveur.

La limite de volumétrie est variable. Dans le cas d'une utilisation sur le serveur de messagerie, une limite de 100Mo est préconisée. Le BCR aura la charge de vérifier et informer l'utilisateur du dépassement de son quota. Dans le cas d'une utilisation hors ligne (disque dur), aucune limite de volumétrie n'est appliquée.

En cas de stockage sur le poste de travail et dans le cas où ce dernier viendrait à tomber en panne, il n'existe aucun moyen de restaurer les emails perdus. Il est donc fortement conseillé, malgré la limite de volumétrie, d'utiliser la messagerie en mode connecté.

Si la boîte aux lettres est stockée sur le serveur, l'agenda est partageable (en lecture et en écriture). L'ensemble des informations est sauvegardé. Toute demande de partage d'agenda devra faire l'objet d'une requête adressée au BCR. L'accès à la boîte aux lettres peut se faire depuis l'extérieur via un Webmail dont l'adresse est disponible sur simple demande auprès du BCR.

Quelle que soit la solution choisie (hors ligne ou en ligne), en aucun cas la boîte aux lettres ne doit servir de lieu de stockage. Les fichiers et les mails sensibles doivent être déplacés dans des répertoires sécurisés dont la gestion incombe à l'utilisateur.

La taille des mails ne peut dépasser 5Mo, pièces jointes incluses, en réception et en émission. Il s'agit d'une limite bloquante. Pour les pièces jointes trop volumineuses, il convient de les envoyer par le biais du service Envol mis à disposition par la DNUM.

C. Accès à internet

Tout utilisateur connecté au réseau bénéficie d'un accès sécurisé à internet et à l'intranet. Cet accès utilise une liaison VSAT qui est mutualisée dans tous les districts et pour tous les personnels et partenaires. Il sert également pour l'interconnexion des différents outils informatiques mis à disposition par les TAAF et partagés sur l'ensemble des territoires qui ne sont pas reliés entre eux par la fibre optique. Les moyens et restrictions cités ci-dessous sont mis en œuvre afin de prendre en compte ces artifices et surtout d'assurer une qualité de service minimale pour les services reliés par ce biais.

Les utilisateurs veilleront à garantir l'intégrité du réseau lors de l'utilisation de services disponibles sur le réseau internet : la composition de l'adresse électronique (URL) engage la responsabilité de l'utilisateur ainsi que celle des TAAF.

Les accès doivent s'effectuer dans un cadre professionnel. Sont proscrits par la loi : la consultation de documents, de textes, d'images ou de sites internet sur la pédophilie, sur des sites à caractère pornographique, raciste, trafic de stupéfiants, …

Afin de respecter la législation, le BCR (sous contrôle du STIR) a mis en œuvre une politique cohérente. Ainsi, la navigation sur internet est limitée par une solution de filtrage d'URL automatique (PFSENSE) qui interdit l'accès aux sites sensibles les plus connus (sites à caractère pornographique, pédophile, raciste…). Ce logiciel émet des états des lieux de la navigation. Le STIR pourra communiquer ces états à la Direction des Ressources Humaines du ministère de l'Intérieur (MI) et aux responsables de services sous couvert du Secrétariat Général du MI. En cas de non-respect de la loi, la décision peut être prise d'isoler le poste de l'utilisateur responsable de l'abus et de prendre toute action disciplinaire ou judiciaire à l'encontre de l'utilisateur concerné.

Afin d'assurer une bonne qualité des services internet et de communication avec les sites distants non reliés par fibre optique, mais aussi pour des raisons de sécurité, sont bloqués :

- Le téléchargement des fichiers multimédias (mp3, vidéos, …) ;
- Les flux liés à des forums de discussions, à des discussions en ligne (chat) ;
- Les abonnements à des listes de diffusion ;
- L'accès aux sites Peer To Peer.

Pour tout besoin spécifique, il conviendra de s'adresser au chef de district qui évaluera le besoin avant de soumettre une demande de modification des filtrages au STIR. Si un utilisateur ne devait pas (ou plus) pouvoir bénéficier de l'accès à internet, le responsable du service doit en aviser le BCR et le STIR par tous moyens écrits.

D. Stockage d'information

Il est tenu à disposition de chaque service une zone de stockage commune des informations sécurisée sauvegardée quotidiennement. Cette zone est stockée sur des serveurs mutualisés pour tous les utilisateurs du réseau dans chaque district. Chaque utilisateur peut y créer l'arborescence qui lui convient mais devra être vigilant sur la taille disque qu'il consomme afin que les autres utilisateurs ne soient pas pénalisés.

Attention

Les accès n'étant pas limités pour les utilisateurs de chaque service, il va de soi que n'importe quel utilisateur peut supprimer les données d'un autre utilisateur sur cet espace commun. La responsabilité du STIR ou du BCR ne pourra être engagée pour les pertes éventuelles de données qui interviendraient sur cet espace de stockage. Il convient donc de ne pas accéder aux données accessibles/disponibles sans en avoir l'autorisation, ni de les supprimer.

La notion de « corbeille » (poubelle) n'existe pas dans cet espace partagé. Les données supprimées le sont définitivement. Une solution de restitution limitée dans le temps et qui nécessite l'intervention du BCR est possible (cf. sauvegarde des données).

Il est interdit de stocker de la musique, des jeux, et autres logiciels « pirates » dans cet espace. Le STIR peut, sans préavis, supprimer tout fichier ne correspondant pas à la présente charte.

Il est possible de limiter les accès de certains dossiers en lecture seule ou totalement. Cette opération sera réalisée par le BCR après saisie d'une demande écrite (courrier détaillé ou demande par mail). Ce courrier sera signé par le responsable de service ou son représentant. Ce courrier devra décrire l'arborescence et les limitations souhaitées.

Le STIR se réserve le droit d'utiliser une gestion de quotas afin d'assurer une bonne qualité du partage et des volumes disponibles.

Une zone de stockage commune à l'ensemble des utilisateurs est accessible depuis chaque poste informatique. Elle est en accès total à tout le monde (lecture / écriture / suppression). Elle a pour vocation de permettre des échanges interservices ponctuels mais ne doit, en aucun cas, servir d'emplacement de stockage des informations. Le STIR ainsi que le BCR déclinent toute responsabilité quant à la perte d'information dans cet espace partagé.

En cas de nécessité, le STIR, par l'intermédiaire du BCR, peut créer des zones spécifiques de stockage de données entre plusieurs utilisateurs de services différents. Dans ce cas, un courrier détaillé (ou un mail) signé par le chef de district ou son représentant devra être transmis au STIR. Ce courrier devra décrire l'arborescence et les limitations souhaitées sur les espaces de stockage du réseau local.

Enfin, dans le cadre de l'amélioration de la communication interdistricts, le STIR met à disposition des espaces de travail partagés afin de faciliter l'échange d'informations. Ce service est accessible sur un espace de stockage en nuage (Cloud Privé) et mis à disposition du siège et de l'ensemble des districts TAAF. Pour en bénéficier, il convient de prendre contact avec le BCR qui formalisera une demande complète au STIR. Ces espaces peuvent être partagés avec des utilisateurs dans les différents districts pour permettre une meilleure coordination des équipes. Compte tenu de l'hébergement en ligne de ces données, il peut être appliqué un quota pour chaque utilisateur.

E. Sauvegarde / restauration des données

Les informations stockées dans les PC en local (disque dur interne ou externe) ne sont pas sauvegardées. Chaque utilisateur veillera à leur sauvegarde autant que besoin. Le STIR et le BCR déclinent toute responsabilité en cas de panne ou de perte de fichier.

Les données stockées sur le réseau (zones de stockage privées et partagées) sont sauvegardées quotidiennement par le BCR. Cette sauvegarde se fait en dehors des heures ouvrées (la nuit). Le BCR assure ainsi une disponibilité de ces données sur 15 jours ouvrés (3 semaines). Sur appel de l'utilisateur, le BCR s'engage à informer l'utilisateur de la disponibilité de ces données sur la sauvegarde sous 30 minutes, et de restaurer ces données sous 2 heures ouvrées.

En cas de problème de sauvegarde (sauvegarde non réalisée ou incomplète), le BCR s'engage à intervenir avant la sauvegarde suivante et à informer le(s) service(s) concerné(s) de la situation.

En cas de crash complet d'un serveur, le BCR s'engage à le réinstaller en l'état sous 24 heures (hors week-end et jours fériés). Les données restaurées seront celles de la dernière version des fichiers sauvegardés.

F. Confidentialité

Les informations stockées sur le réseau ou dans les postes de travail sont accessibles à tous les personnels du BCR et du STIR pour des raisons de maintenance. Les techniciens du BCR et du STIR ne sont pas autorisés à consulter ou à diffuser ces informations sauf si le service ou l'utilisateur concerné en fait la demande (pour une aide bureautique par exemple). En cas de doute sur la demande exprimée par l'utilisateur, le technicien se réserve le droit de consulter le responsable du service concerné ou son représentant, ainsi que le chef de district pour s'assurer du respect de la présente charte.

Le STIR et le BCR installent des logiciels de prise en main à distance pour pouvoir intervenir plus rapidement en cas de besoin sans se déplacer. Les techniciens du STIR et du BCR ne pourront utiliser ces outils qu'avec l'accord de l'utilisateur concerné. Un accord oral suffira.

Les personnels techniques du STIR et du BCR disposent d'habilitations spécifiques afin de traiter des données sensibles. Ils s'engagent en outre à respecter scrupuleusement les règles et lois en matière de vie privée et de confidentialité. Ils ne peuvent communiquer à quelque tiers que ce soit les informations dont ils auraient connaissance dans l'exercice de leurs fonctions.

Pour les utilisateurs nécessitant un haut niveau de confidentialité (chef de district, médecin, …), le STIR met à disposition sur demande écrite des comptes Nomade 2.0 (messagerie hautement sécurisée mise en œuvre par le Ministère de l'Intérieur).

G. Le réseau

Pour des raisons de sécurité, aucune connexion distante concurrente n'est tolérée : l'accès à internet se fait exclusivement au travers du lien VSAT mutualisé des TAAF. Tous les accès à des bases de données distantes via internet feront l'objet d'une demande au STIR et d'une analyse technique approfondie. L'utilisation de VPN sur les postes professionnels comme en libre-service ne sont pas autorisées sauf accord express du STIR.

H. Numéro d'appel

En cas de panne ou anomalie informatique, l'utilisateur pourra appeler le numéro suivant :

- Terre Adélie : 2022
- Amsterdam : 3022
- Kerguelen : 4022
- Crozet : 5022

I. Réglementation en vigueur

Il convient à tous les utilisateurs de se conformer aux lois et textes en vigueur concernant les droits d'auteur, la sécurité informatique, l'informatique et les libertés, l'usage de la langue française et le téléchargement illégal en prenant connaissance des textes suivants :

- Loi n°78-17 du 6 janvier 1978 (dite loi informatique et libertés)
- Loi n°88-19 du 5 janvier 1988 (dite loi Godfrain)
- Loi n°94-665 du 4 août 1994 (dite loi Toubon)
- Loi n°2004-575 du 21 juin 2004 (dite loi pour la confiance dans l'économie numérique)
- Loi n°2009-1311 du 28 octobre 2009 (dite loi Hadopi 2)

J. Téléchargements illégaux : Rappel

Pour ce qui est de la copie et de la diffusion publique ou privée d'œuvres cinématographiques ou musicales, il est rappelé que la mise à disposition de films ou musiques en libre-service sur un serveur et accessibles au téléchargement sur tout ordinateur connecté au réseau informatique est illégale.

Le Code de la Propriété Intellectuelle précise en effet que : « Toute édition d'écrit, de composition musicale, de dessin, de peinture ou toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit. » ; « Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur… ».

En conséquence, tout téléchargement d'œuvres concernées par cet article est strictement interdit.

K. Réseaux sociaux et applications de messagerie instantanée

Il est rappelé que le réseau informatique est déployé dans les districts pour les besoins professionnels prioritairement. A ce titre, il est totalement interdit d'utiliser des réseaux sociaux et des outils de messagerie instantanée sur les postes informatiques professionnels.

Pour se connecter à ces outils et garder le contact avec sa famille et ses amis, des postes informatiques « libre-service » ainsi qu'une borne WiFi dédiée à cet usage sont mises en œuvre dans chaque district.

Il est conseillé à l'utilisateur de se renseigner auprès du BCR afin de connaître les modalités d'accès à ces postes en libre-service. L'utilisation de ces moyens partagés est encadrée par une note de service.

4. La téléphonie

Le réseau téléphonie des TAAF est vaste et complexe. Il est composé d'un système basé sur un autocom centralisé situé au siège des TAAF à Saint-Pierre qui est interfacé à un opérateur de téléphonie pour assurer les communications vers la téléphonie fixe, 5 autocoms déportés (Terre Adélie, Amsterdam, Kerguelen, Crozet, Paris) via une liaison VSAT ou via Internet pour Paris. Ces autocoms déportés ne sont pas autonomes en cas de coupure de la liaison vers le siège des TAAF et ne permettent que les communications internes dans chaque district.

Une solution technique de limitation des coûts vers les téléphones fixes des autres districts, du siège ou de l'antenne parisienne a été mise en œuvre. Il s'agit d'une solution de convergence qui permet d'appeler au travers de numéros abrégés des téléphones fixes en minimisant les coûts.

A. Restrictions

Par défaut, toute ligne téléphonique fixe est restreinte :

- Restriction géographique (appels internes, locaux, régionaux, nationaux ou internationaux)
- Restriction d'accès depuis l'extérieur (Sélection Directe à l'Arrivée : SDA)

Les autocoms, eux aussi, sont restreints :
- Terre Adélie : 8 appels extérieurs en simultané ;
- Amsterdam : 5 appels extérieurs en simultané ;
- Kerguelen : 5 appels extérieurs en simultané ;
- Crozet : 3 appels extérieurs en simultané ;
- Paris : 6 appels téléphoniques extérieurs en simultané.

Tout souhait d'évolution de la configuration d'une ligne téléphonique ou d'attribution d'un numéro direct devra se faire auprès du BCR par écrit (ou par mail) qui procédera à la mise en place après accord du STIR.

B. Règles en vigueur

L'utilisateur s'engage à respecter quelques règles d'usage :
- Les échanges doivent être professionnels ;
- Un téléphone fixe ne peut pas être déplacé sans l'intervention du BCR ;
- Il convient de privilégier les appels vers des numéros abrégés pour les appels vers d'autres districts ou le siège ;
- Il est interdit d'appeler des services du type « téléphone rose » ou de chat ;
- Les équipements mis à disposition des utilisateurs ainsi que tous leurs accessoires sont la propriété des TAAF, il est donc du devoir des personnels d'en prendre le plus grand soin ;
- Les appels vers l'étranger sont interdits, sauf motif de service ;
- Les abus constatés feront l'objet d'une facturation par le BCR au tarif en vigueur (cf. arrêté préfectoral n°2019-167 du 14 novembre 2019 portant sur l'utilisation de la téléphonie dans les districts).

C. Confidentialité

Aucun équipement n'est surveillé. Cependant, la facturation détaillée précise la liste des appels, leur durée et leur destination. Ces listes sont consultées par le BCR à des fins de facturation. Le BCR se réserve le droit d'alerter le responsable du service concerné par des abus et de refacturer ces communications au personnel concerné.

D. Boîte vocale

Il est possible de bénéficier d'une boîte vocale pour les sites reliés aux différents autocoms. Le système de boites vocales est mutualisé pour chaque autocom. Toute demande de mise en place d'une boite vocale doit faire l'objet d'une demande écrite auprès du BCR qui procédera à sa mise en service après validation par le STIR.

E. Numéro d'appel

En cas de panne ou d'anomalie de téléphonie, l'utilisateur peut appeler le numéro suivant :
- Terre Adélie : 2022
- Amsterdam : 3022
- Kerguelen : 4022
- Crozet : 5022

En cas de panne générale, il convient d'alerter au plus vite le BCR qui effectuera les travaux de maintenance corrective en liaison avec le STIR.

5. La radio

Dans chaque district, des moyens de communication radio sont mis en place. La radio est un moyen de communication instantané et à faible coût sur les bases et sur tout ou partie des territoires. C'est un élément indispensable à la sécurité des personnels. La radio permet en outre d'assurer le bon déroulé des opérations logistiques.

Pour garantir une efficacité optimale de cet outil, des procédures strictes doivent être respectées de la part des usagers.

Il existe plusieurs types de communication radio, les moyens déployés dans les territoires sont la Très Haute Fréquence (VHF) et l'Ultra Haute Fréquence (UHF).

A. VHF

Les fréquences VHF voyagent plus loin si elles ne sont pas perturbées par des barrières ou obstacles naturels. Elles sont largement utilisées lors des sorties en dehors de la base. Elles peuvent être perturbées par d'autres ondes radio. L'utilisation de radios VHF est optimale dans des étendues sans obstacle (bâtiment, végétation dense, haut relief, …).

Pour assurer le bon fonctionnement en dehors de la base, des relais radio sont mis en place sur les points hauts des districts. Ils sont maintenus en état de bon fonctionnement par le BCR qui procède aux vérifications d'usage et au changement des batteries plusieurs fois par an.

Des radios portatives VHF sont à disposition au BCR. Il incombe à chaque usager de se renseigner préalablement auprès du BCR pour les formalités d'emprunt. En cas de dégradation ou perte du matériel, il convient de signaler immédiatement au BCR la nature du problème, ceci afin de permettre un remplacement rapide du matériel et ne pas compromettre la sécurité des personnels pour les futures manips.

La dégradation ou la perte du matériel radio doit faire l'objet d'un compte rendu manuscrit, daté et signé par l'usager. Ce compte rendu sera remis au BCR lors du signalement. Il est essentiel de respecter cette procédure de signalement afin de garantir la bonne prise en compte par le BCR et par le STIR des dégâts occasionnés au matériel et leurs circonstances.

Seul le BCR est habilité à procéder à des changements et des réparations sur les radios portatives (remplacement de batterie ou d'antenne). Ils disposent d'une formation spécifique qui permet de garantir le fonctionnement pérenne du matériel.

B. UHF

Les fréquences UHF sont intéressantes pour les longues distances. L'UHF est un moyen plus adapté lorsque vous utilisez des radios en intérieur ou dans un milieu avec de nombreux obstacles naturels (bâtiments, forêt, …). Les radios UHF sont moins sensibles aux perturbations d'autres ondes radio.

C'est donc un moyen essentiellement utilisé lors des opérations portuaires. L'UHF permet de communiquer avec le Marion Dufresne sans subir de dégradation de signal.

Comme pour les radios portatives VHF, seul le BCR est habilité à procéder à des modifications (changement de batterie ou d'antenne) afin de garantir le fonctionnement optimal de ces appareils.

C. Règles d'usage

Les radios VHF et UHF évoluant sur des gammes de fréquences différentes, il n'est pas possible de communiquer entre VHF et UHF.

Tous les membres d'une mission sont susceptibles d'utiliser une radio. Il est donc essentiel d'être formé aux bons usages de cet outil.

La formation est réalisée dans chaque district par le chef du BCR sous l'autorité du chef de district. Ces derniers ont été formés au préalable par un technicien télécom du STIR lors de la préparation à l'hivernage.

Il est important que chaque participant à une mission connaisse les règles élémentaires pour la gestion du trafic radio. Ces règles de base sont :

- Utilisation d'un canal principal et possibilité de basculer sur d'autres canaux ;
- Identification claire de l'émetteur et du récepteur ;
- Concision, précision et clarté de l'expression ;
- Restitution de l'information ou de l'ordre lorsque le message est important ou ambigu.

Tant que possible, il est recommandé de se rapprocher des procédures radio militaires.

Cette discipline est impérative lors des OP, mais également durant toute la durée des missions.

Le chef du BCR et, si besoin, le chef de district ont toute autorité pour rappeler à l'ordre les personnels ne respectant pas les consignes (les bavardages sont prohibés).

Le succès d'une opération (logistique, technique, sortie de base, …), mais aussi et surtout la sécurité des personnes, repose sur une bonne utilisation des moyens de communication radio.

Des radios sont mises à disposition par le BCR. L'emprunt des radios engage la responsabilité des usagers. Toute perte ou dégradation de matériel doit être signalée immédiatement au BCR. Il incombera à l'usager d'émettre un compte rendu complet, manuscrit, détaillant précisément les circonstances de cette perte ou dégradation.

Comme annoncé précédemment, seul le BCR est habilité à procéder à un changement de batterie, d'étui ou d'antenne, ceci afin de garantir la pérennité des matériels.

En cas de départ pour une manip de longue durée, une dérogation peut être demandée au BCR par tout moyen écrit afin de recevoir une batterie de secours. Le BCR formera l'usager afin qu'il puisse procéder par lui-même au changement de la batterie.

D. Listes des indicatifs

Indicatif	**Signification**
OPEA	Chargé des Opérations des Expéditions Australes
DZ	Responsable de l'aire de poser hélicoptère à terre
LA CALE (Amsterdam) **LA PLAGE (Crozet)** **LE PORT (Kerguelen)**	Responsable de la cale dur le district
PORT PETROLIER	Responsable du port pétrolier
L'AVENTURE	Pilote du chaland
SECOND	Second capitaine du Marion Dufresne
HELICO	Pilote de l'hélicoptère
DISAMS (Amsterdam) **DISCRO (Crozet)** **DISKER (Kerguelen)**	Chef de district
TOURISTE	Guide touristique
BCR	Bureau Communication Radio
MEDECIN	Médecin du district
Nom du site de mission	Equipe en mission sur le terrain Exemple : Pointe Basse, BUS, Château, Entrecasteaux, …

E. Allocation de fréquences

Les fréquences sont allouées par le BCR de chaque district, sous la supervision du STIR, qui est chargé de la surveillance du trafic. Le chef de district a autorité pour interdire l'accès de certains personnels aux fréquences de travail.

Par principe, les fréquences suivantes sont attribuées lors des opérations portuaires :

- Canal 6 : OPEA
- Canal 8 : Sécurité base
- Canal 9 : Hélicoptère
- Canal 10 : Bateaux de pêche
- Canal 12 : Canal de travail
- Canaux 26 et 27 : Intérieur du district et lorsque l'hélicoptère est de portée de VHF

F. Communications

Les termes suivants sont utilisés de façon courante :

ICI…	Cette transmission vient de la station dont la désignation vient immédiatement après…
PARLEZ	Ceci est la fin de ma transmission pour vous, j'attends votre réaction, je vous écoute
PARLEZ PLUS LENTEMENT	Réduisez votre vitesse de transmission
JE REPETE	Je répète la transmission
ATTENDEZ	Je dois stopper ma transmission pendant quelques secondes
SILENCE	Cessez immédiatement toute transmission sur ce réseau
TERMINE	Ceci est la fin de ma transmission pour vous et je n'attends aucune réponse de votre part
RECU	J'ai bien reçu votre dernière transmission
REPETEZ	Répétez toute votre dernière transmission
CORRECTION	Une erreur a été faite dans cette transmission, la version correcte est la suivante…

Exemples :
« OPEA, ICI HELICO. J'attends vos instructions. PARLEZ »
« HELICO, ICI OPEA. Restez en attente. TERMINE »

G. Contrôles radio

Les contrôles radio permettent d'évaluer la force et la lisibilité du signal.

CONTROLE RADIO	Comment m'entendez-vous ?
RECU	J'ai reçu votre dernière transmission de manière satisfaisante
RIEN ENTENDU	A utiliser si aucune réponse ne parvient de la station appelée
FORT	Le signal est très fort
ASSEZ FORT	Le signal est bon
FAIBLE	Le signal est faible
TRES FAIBLE	Le signal est très faible
CLAIR	Excellente qualité de la voix
LISIBLE	Qualité de la voix satisfaisante
ILLISIBLE	Qualité de la voix inaudible
DEFORME	Voix déformée
AVEC INTERFERENCE	Voix couverte par des interférences
INTERMITTENT	Voix hachée

Exemples :
« OPEA, ICI HELICO pour CONTROLE RADIO. PARLEZ »

« HELICO, ICI OPEA. Reçu FORT et CLAIR. TERMINE »

H. Confidentialité

Les radios VHF et UHF fonctionnent sur des fréquences hertziennes ouvertes et non cryptées. Il est donc évident qu'il n'y a sur cet outil de communication aucune sécurité et que les seuls filtres appliqués à la communication sont ceux de l'usager.

Nous vous demandons donc la plus grande prudence dans les propos échangés sur les radios HF. En effet, un bateau posté au large pourrait tout à fait intercepter une communication, sciemment ou de manière fortuite.

Les échanges et transmissions radio ne doivent jamais comporter d'informations sensibles.

[Document à parapher et à signer]

Fait à : **Le :**

Statut :

Lieu d'affectation :

Date d'affectation :

Certifie avoir pris connaissance de la présente charte d'utilisation des services et ressources informatiques et de communication.

Signature :