



**PRÉFET
ADMINISTRATEUR SUPÉRIEUR
DES TERRES AUSTRALES
ET ANTARCTIQUES
FRANÇAISES**

*Liberté
Égalité
Fraternité*

Charte internet s'appliquant aux districts des Terres australes antarctiques françaises (TAAF) et aux rotations sur le Marion Dufresne organisées par les TAAF

PREAMBULE :

Cette charte est à destination de toute personne demandant un accès internet professionnel et/ou personnel aux réseaux maîtrisés des TAAF sur les districts (districts austraux, terre Adélie et îles Eparses), et aux rotations sur le Marion Dufresne organisées par les TAAF. Pour bénéficier du service d'accès à internet, vous devez prendre connaissance des conditions d'utilisation fixées par cette charte, et les accepter en signant l'engagement personnel figurant dans ce document.

Tout abus ou infraction engage la responsabilité de l'utilisateur et fera l'objet de sanctions (suspension ou clôture du compte Internet, information de l'autorité hiérarchique, et sanctions disciplinaires voire poursuites si nécessaire).

Les chefs de district peuvent compléter cette charte par des règles de bonnes pratiques afin que l'usage d'internet ne nuise pas à la vie de groupe et à la cohésion de la mission.

1. Gestion des connexions

a. Traitement statistique

Le STIR et le BCR procèdent à une analyse quotidienne de l'usage qui est faite d'Internet à des fins de sécurité et de statistiques, en suivant la consommation quotidienne de données de chaque compte nominatif. Chaque titulaire de compte peut accéder à ces informations via un portail.

b. Application de la politique internet et du niveau de sécurité

Sur les réseaux TAAF-PRO et TAAF-public, le STIR et le BCR peuvent mettre en œuvre des politiques de filtrage afin :

- De bloquer des usages individuels contraires à la charte Internet ou à la politique de sécurité des systèmes d'information ;
- De détecter toute manifestation d'une éventuelle attaque informatique.

c. Conservation des données, droit d'accès et de rectification

Conformément à l'article L34-1 du code des postes et des communications électroniques, les données techniques de connexion sont conservées pendant un délai de un an à compter de la connexion. Les informations relatives à l'identité civile de l'utilisateur sont conservées pendant un délai de 5 ans. Les utilisateurs disposent d'un droit d'accès et d'un droit de rectification, en contactant le délégué à la protection des données.

2. Conditions d'utilisation sur les districts pour les personnels du district

L'accès Internet est mis à disposition dans un cadre professionnel sur les réseaux professionnels dénommés « **TAAF-PRO** » accessibles uniquement par des équipements fournis par le STIR ou le BCR.

Un usage personnel est permis uniquement sur les réseaux sans-fils et sur les postes internet mis à disposition par le BCR dénommés « **TAAF-PUBLIC** », et à la stricte condition de respecter les conditions fixées ci-dessous. La priorité est toujours donnée à l'accès internet à des fins professionnelles.

a. Usage professionnel

Usage Professionnel TAAF-PRO	Recouvre toutes les consultations en relation directe avec un besoin professionnel.
Précaution	Maintenir un usage quotidien raisonnable et en rapport avec l'activité professionnelle. Toujours fermer le navigateur après avoir obtenu l'information souhaitée. Éviter de télécharger des fichiers volumineux (supérieurs à 10 Mo) en heures de pointe (08h-12h et 14h-18h). Privilégier l'usage de Nextcloud pour partager des fichiers.
Quota	Le téléchargement est limité aux fichiers d'une taille maximale de 100 Mo.
Emplacement	Sur les lieux de travail
Interdictions	Se référer au 4.

Si votre activité professionnelle vous contraint à une consommation supérieure au quota défini ci-dessus, il est conseillé d'en faire part au STIR ou au BCR.

b. Usage personnel

Usage Personnel TAAF-PUBLIC	Seule une utilisation relevant de la vie courante est tolérée. L'utilisateur est attentif à ce que celle-ci demeure raisonnable et ne mette pas en péril les conditions d'accès professionnel au réseau. Tout abus engage la responsabilité du titulaire du compte.
Précaution	Toujours fermer le navigateur après avoir obtenu l'information souhaitée. Consulter de façon courte les messageries instantanées de ses réseaux sociaux. Couper le wifi entre deux utilisations pour éviter une consommation incontrôlée.
Quota	<u>Consommation individuelle mensuelle maximale sur les districts et à bord du Marion Dufresne</u> : 4.5 Go par mois (le seuil pourra être adapté par le STIR en fonction de la consommation du district), ce qui représente une moyenne quotidienne de 150 Mo. La bande passante est encadrée par le STIR et le BCR pour la partager équitablement et préserver la fluidité du réseau internet, en priorisant TAAF-PRO.
Emplacement	Chambres (lieu privé) / lieux de vie communautaires dotés d'une borne wifi
Authentification	Authentification personnelle avec l'identifiant et le mot de passe fournis par le BCR
Interdictions	Se référer au 4.

3. Conditions d'utilisation pour tous les agents à bord du Marion Dufresne, et pour les visiteurs et interdistrict sur les districts

Les visiteurs et interdistricts, ainsi que tous les agents à bord du Marion Dufresne, peuvent bénéficier d'un accès internet à l'usage personnel et professionnel mais le quota est plus restrictif que pour les personnels du district (paragraphe 2.) afin d'assurer la bonne continuité des missions.

Usage Personnel TAAF-PUBLIC	Seule une utilisation relevant de la vie courante est tolérée. L'utilisateur est attentif à ce que celle-ci demeure raisonnable et ne mette pas en péril les conditions d'accès professionnel au réseau. Tout abus engage la responsabilité du titulaire du compte.
Quota	<u>Consommation individuelle quotidienne maximale : 100 Mo par jour</u> (le seuil pourra être adapté par le STIR en fonction de la consommation du district) La bande passante est encadrée par le STIR et le BCR pour partager équitablement celle-ci et préserver la fluidité du réseau internet, en priorisant le réseau TAAF-PRO. <u>Pour les partenaires</u> : le quota est défini en fonction de la convention signée avec les TAAF. A défaut d'une mention spécifique, le quota de 100 Mo s'applique.
Interdictions	Se référer au 4.

Usage Professionnel TAAF-PRO	Toutes consultations en relation directe avec un besoin professionnel. Utilisation d'un poste NOEMI OU NOMADE pour les agents du siège des TAAF
Quota	Le téléchargement est limité aux fichiers d'une taille maximale de 100 Mo.
Filtrage autorisé	S'appuie sur la charte ORION émise par le centre de la cyberdéfense du ministère de l'intérieur pour les agents du siège des TAAF.
Contournement de la politique de filtrage	VPN RIE autorisé
Interdictions	Se référer au 4.

4. Usages interdits

<p>Usage Interdit</p>	<p>Lorsqu'ils sont découverts, les sites au contenu illégal ou mettant en danger la sécurité du système d'information des TAAF sont inscrits sur une liste noire les rendant inaccessibles depuis les réseaux des TAAF.</p> <p>Si vous constatez un site accessible entrant dans une de ces catégories, informez immédiatement le STIR ou le BCR. La possibilité technique de consulter un site ne vaut pas autorisation.</p> <p>Tout abus engage la responsabilité du titulaire du compte.</p>
<p>Sites au contenu illégal</p>	<p>Pédophiles, Négationnistes, Vente de produits interdits (armes, drogues...), Escroquerie, imitation/détournement de sites, Provocation ou apologie des actes de terrorisme, des crimes de guerre, crimes contre l'humanité, ... Incitation à la discrimination, à la haine ou à la violence raciale, ... Diffusion d'œuvres protégées par les droits d'auteur, Outils de piratage informatique, logiciels contrefaits ou piratés, Tout autre site au contenu illégal</p>
<p>Danger pour le système d'information</p>	<p>Site hébergeant du code malveillant (virus informatique). Pour votre bonne information, les sites hébergeant du contenu pour adulte diffusent très souvent des virus informatiques. Ports réseau non standards (différents de 80, 443, ...) Prise de main distante, VPN, ... Sites litigieux pouvant être en relation avec une escroquerie Sites entraînant une surcharge majeure du service Internet Installation de logiciels et d'extensions de navigateurs non qualifiés Tout autre site présentant un danger pour le système d'information</p>
<p>Sécurité, et ralentissement du service Internet</p>	<p>Le STIR et le BCR se réservent le droit d'interdire l'accès à tout site dont le taux de charge induite est fort, où la sécurité informatique peut impacter le réseau TAAF et dont l'intérêt pour les missions n'est pas essentiel.</p> <p>Exemple : la lecture de flux audio et vidéo diffusé en « direct » ou en léger direct (streaming) n'est pas autorisée.</p>
<p>Contournement de la politique de filtrage</p>	<p>Site de redirection/masquage (proxy) VPN (à l'exception du VPN RIE pour les personnels du siège)</p>

Récapitulatif des conditions d'utilisations :

- **L'usage d'internet relève de votre responsabilité personnelle.** Vous ne devez pas communiquer vos identifiants à un tiers, même à des fins professionnelles ;
- Vous devez verrouiller votre session en votre absence ;
- Les actions de navigation et de téléchargement effectuées sur Internet sont tracées et font l'objet de contrôles et de statistiques ;
- Le suivi de votre consommation Internet est disponible sur le portail d'accès à votre compte Internet. Vous pouvez aussi y changer votre mot de passe ;
- L'accès vous est fourni à **des fins professionnelles** et personnelles, pour une utilisation loyale. Le trafic généré doit rester raisonnable et seule une utilisation relevant des nécessités de la vie courante, ne nuisant pas à l'activité des services, est tolérée ;
- La possibilité technique de consulter un site ne vaut pas autorisation. Sont interdits les sites dont le contenu est contraire à la loi française et ceux qui peuvent toucher la sécurité et la réputation de l'institution ;
- La divulgation d'informations professionnelles sur vous-même ou votre service en dehors de la sphère professionnelle (adresses de messagerie...) est interdite, pour éviter de faciliter une cyberattaque ciblée ;
- Les sites et les documents récupérés sur internet peuvent être piégés. Soyez vigilant lorsque vous naviguez ;
- Informez le BCR de tout problème ou comportement anormal de votre ordinateur. N'hésitez pas à le contacter pour toute demande de précision.

De plus amples renseignements sont disponibles auprès du STIR et du BCR.

Les abus seront sanctionnés (suppression immédiate des accès, sanction disciplinaire).

Des poursuites seront engagées si nécessaires.

Engagement personnel

Je, soussigné :

Nom : Prénom :

Certifie avoir pris connaissance de la présente charte internet s'appliquant aux districts des Terres australes antarctiques françaises et accepte d'en appliquer les principes lors de mon séjour sur les districts.

Et déclare avoir pris connaissance des sanctions disciplinaires et pénales encourues en cas de non-respect de cette dernière.

Fait le : à

Signature :

(Parapher toutes les pages)

ANNEXE

Pourquoi une nécessaire vigilance dans l'usage d'internet ?

Les adresses de courriels font l'objet d'un véritable marché. Elles sont recherchées et revendues pour envoyer des courriels indésirables.

La diffusion d'informations facilite l'ingénierie sociale : les informations recueillies sur les personnes et leurs fonctions, les structures ou les projets peuvent servir à tromper un correspondant dans le but de lui soutirer des informations sensibles ou de lui faire parvenir un courriel piégé crédible qui sera ouvert sans méfiance.

Le recoupement d'information entre vie privée et vie professionnelle peut nuire à l'image de l'administration ou mettre en danger l'agent et sa famille.

Tous les jours des sites internet se font pirater et les informations relatives à leurs clients ou lecteurs sont divulguées. Lorsque des mots de passe sont réutilisés dans plusieurs contextes différents, un attaquant peut étendre une compromission à d'autres systèmes.

Documents piégés

Lorsque vous téléchargez ou consultez un document sur internet, un contrôle antivirus est effectué. Pour qu'un virus soit arrêté, il doit d'abord avoir été identifié comme tel par l'antivirus. Il peut donc exister un moment pendant lequel les TAAF ne sont pas protégés d'un virus inconnu.

L'ouverture d'un document piégé peut compromettre votre poste de travail. Vos données peuvent être supprimées, ou être copiées par l'attaquant. Il est également possible d'enregistrer et transmettre les frappes du clavier ou des captures d'écran. Le code malveillant peut se propager ensuite par les clefs USB, par le réseau ou par la messagerie.

En cas de comportement anormal de votre poste de travail, contactez votre RSSI (BCR pour les agents des districts et STIR pour les personnes du siège).