

## **POLITIQUE D'USAGES AUTORISÉS PAR GLOBAL CROSSING**

**AOÛT 2006**

### **CONDITIONS GÉNÉRALES D'UTILISATION**

**1.1** Tous les clients Global Crossing sont tenus de consulter et d'appliquer la présente Politique d'Usages Autorisés. Les clients Global Crossing fournissant des services à leurs propres clients ou utilisateurs finaux se portent garants du respect par leurs utilisateurs finaux des dispositions de cette Politique et s'engagent à prendre des mesures à cet effet. Aux fins de la présente Politique, « Client » désigne tout client Global Crossing bénéficiant de services Global Crossing, ainsi que l'ensemble du personnel, des agents et des tiers auprès desquels le Client rend les services Global Crossing disponibles. Global Crossing se réserve le droit de refuser ou de résilier la fourniture de services à un Client au vu des résultats de la procédure de vérification de sécurité/d'utilisation abusive mise en œuvre par Global Crossing. Cette procédure examine notamment, à l'aide d'informations publiquement disponibles, l'utilisation passée et actuelle par le Client de services similaires à ceux fournis par Global Crossing et l'historique de ses relations avec ses précédents fournisseurs.

**1.2** Les pratiques décrites ci-dessous, définies par Global Crossing comme des « utilisations abusives du réseau », sont strictement interdites aux termes de la présente Politique d'Usages Autorisés. Il s'agit d'exemples non exhaustifs, fournis uniquement à des fins d'information. En cas de doute quant à la légitimité d'une utilisation ou d'une activité envisagée, le Client sera tenu de vérifier si cette utilisation est autorisée en contactant Global Crossing par courrier électronique. Les pratiques visées ci-après sont expressément proscrites et Global Crossing se réserve le droit discrétionnaire de mettre en œuvre toutes mesures qu'il estime légitimes, y compris notamment, l'émission de mises en garde verbales ou écrites, le filtrage, le blocage, la suspension ou la résiliation des comptes, l'application de frais d'administration et/ou de coûts de réactivation ou l'introduction de poursuites légales, pour obtenir la cessation des manquements et/ou l'octroi de dommages et intérêts pour les éventuels préjudices causés de ce fait. Global Crossing pourra prendre ces mesures sans obligation de préavis à l'égard du Client. De manière générale, les Clients Global Crossing doivent s'abstenir de faire du réseau, des équipements ou des services Global Crossing une utilisation ayant pour effet de :

- contrevenir aux lois, réglementations, traités ou conventions applicables, y compris notamment les dispositions légales relatives à la confidentialité des données ;
- violer les politiques d'usages autorisés des réseaux, équipements ou services accessibles par le réseau Global Crossing ;
- enfreindre les droits de propriété intellectuelle de Global Crossing ou d'autres personnes ;
- violer les droits de confidentialité d'autres personnes ;
- entraîner la revente de produits ou services Global Crossing, sauf si cette revente est dûment documentée sous forme d'accord écrit spécifique ou dans le cadre du contrat initial signé entre le Client et Global Crossing ;
- donner lieu à des pratiques commerciales trompeuses sur Internet, notamment au regard des recommandations émises par le *United States Federal Trade Commission* dans ce domaine ;
- contrevenir à des instructions spécifiques de Global Crossing destinées à préserver la santé, la sécurité ou la qualité d'autres services de télécommunications fournis par Global Crossing ou à assurer la compatibilité technique d'un équipement associé au Réseau Global Crossing ;
- compromettre substantiellement la qualité d'autres services de télécommunications fournis par Global Crossing ; ou
- manquer de toute autre manière à la présente Politique d'Usages Autorisés.

**1.3** Sont également proscrites, sans que cette liste soit exhaustive, les activités suivantes :

- utilisation non-autorisée (y compris toute tentative à cet effet) ou sabotage d'ordinateurs, de machines ou de réseaux ;
- tentative d'interférence ou de refus de service à un utilisateur ou un site hôte (par exemple, attaques en refus de service et/ou d'usurpation DNS) ;
- falsification d'informations d'identification utilisateur ;
- introduction de programmes malveillants dans le réseau ou sur le Serveur (par exemple, virus, vers, chevaux de Troie, etc.) ;
- recherche non-autorisée des vulnérabilités de réseaux tiers ;
- conduite d'activités de monitoring réseau quelles qu'elles soient (par exemple, à l'aide d'un analyseur de paquets) ou de toutes autres activités visant à contrôler ou intercepter sans autorisation des données non destinées au Client ;
- tentative de contournement du système d'authentification client ou du dispositif de sécurité de tout site hôte, réseau ou compte (méthode dite de « cracking ») sans autorisation ;
- utilisation de programmes/scripts/commandes ou envoi de messages destinés à interférer avec une session terminal d'un tiers par quelque moyen que ce soit, localement ou par Internet ;
- hameçonnage (« phishing »), à savoir pratique consistant à simuler des communications avec le site Web ou d'autres services d'une entité pour recueillir des données d'identification, des habilitations de sécurité et d'autres informations auprès d'utilisateurs légitimes dudit service ;
- pratique dite de « pharming », consistant à utiliser des programmes malveillants, des systèmes d'infection des caches DNS ou d'autres moyens pour rediriger un utilisateur sur un site Web ou un autre service simulant celui d'une entité légitime afin de recueillir des données d'identification, des habilitations de sécurité et d'autres informations auprès des utilisateurs légitimes du service et permettant la transmission, la réception, le téléchargement, l'utilisation ou la réutilisation de contenus illégaux, indécents, diffamatoires, obscènes, menaçants ou violant les droits d'auteur, de confidentialité, de protection des données ou autres droits de tiers ;
- fourniture de données fausses ou inexactes sur le formulaire d'inscription ; ou
- tentative visant à contourner ou altérer les processus ou procédures de mesure des temps de visite et d'usage de bande passante ou les autres méthodes utilisées pour documenter « l'usage » des produits et services Global Crossing.

**1.4 Politique « Digital Millennium Copyright Act » :**

Global Crossing s'efforce de répondre dans les meilleurs délais aux allégations de violation de propriété intellectuelle. Global Crossing traitera et examinera rapidement les infractions notifiées et prendra les mesures appropriées prévues aux termes de la loi « Digital Millennium Copyright Act » (la Loi « DMCA ») et d'autres lois applicables de protection de la propriété intellectuelle. Dès réception d'une réclamation relevant (parfaitement ou substantiellement) de la Loi DMCA, Global Crossing s'efforcera, si cela est en son pouvoir, de supprimer ou de désactiver dans les meilleurs délais l'accès au contenu prétendument contrefaisant ou supportant une activité de contrefaçon et de supprimer ou de désactiver l'accès aux références et liens relatifs au contenu ou à l'activité incriminée. Global Crossing résiliera l'accès des Clients ayant commis des infractions répétées. Les Clients ayant souscrit des services de transit IP, d'accès Internet dédié et de colocalisation doivent adopter et mettre en œuvre une politique Digital Millennium Copyright Act prévoyant la possibilité de retirer ou de désactiver tout contenu contrefaisant. Si vous estimez qu'une œuvre protégée a été copiée et que cette copie est disponible sur notre site sous une forme constitutive de contrefaçon, vous pouvez nous en informer en fournissant à notre collaborateur désigné en charge des questions de droits d'auteur les informations suivantes :

- signature électronique ou physique de la personne autorisée à agir pour le compte du titulaire des droits d'auteur ;
- description de l'œuvre protégée prétendument contrefaite ;
- description de l'emplacement du contenu prétendument contrefaisant sur le site ;
- votre adresse, numéro de téléphone et adresse e-mail ;
- déclaration selon laquelle vous croyez de bonne foi que l'utilisation litigieuse n'a pas été autorisée par le

- titulaire des droits d'auteur ou son agent ou est contraire à la loi ; et
- déclaration sous peine de parjure attestant que les informations figurant dans votre notification sont exactes et que vous êtes le titulaire des droits d'auteur ou son représentant autorisé.

**1.5** Les violations de droits d'auteur doivent être notifiées par e-mail à [dmca@gblox.net](mailto:dmca@gblox.net). Lorsque Global Crossing supprime ou désactive l'accès à un contenu prétendument contrefaisant, Global Crossing peut tenter de contacter le Client à l'origine de sa mise en ligne pour lui permettre de répondre à la mise en cause. Toutes les réponses soumises par le Client incriminé seront communiquées à l'émetteur de la réclamation. Global Crossing donnera à l'émetteur de la réclamation l'opportunité de faire valoir ses droits en justice tel que prévu par la Loi DMCA, avant de réactiver ou de restaurer l'accès à un contenu sur la base des éléments apportés en réponse par la partie mise en cause.

## **2. DISPOSITIONS SUPPLÉMENTAIRES APPLICABLES AUX SERVICES TRANSIT IP, ACCÈS INTERNET DÉDIÉ ET IP**

**2.1** Outre les Conditions Générales d'Utilisation visées ci-dessus, les dispositions du présent Article 2 s'appliqueront à l'utilisation des Services Transit IP, Accès Internet Dédié et IP de Global Crossing. Sont notamment proscrites les activités suivantes :

- falsification d'informations d'en-tête ou de données d'identification utilisateur ;
- atteintes à la sécurité (tentées ou abouties) ou à la communication Internet notamment en accédant à des données dont le Client n'est pas destinataire ou en se connectant à un Serveur ou un compte auquel le Client n'est pas expressément autorisé à accéder ;
- détournement d'espace IP ;
- envois massifs d'e-mails non-sollicités (« opt-out ») ;
- maintien d'un relais de messagerie et/ou d'un proxy ouvert ;
- recueil d'adresses e-mail sur Internet dans le but d'effectuer des envois massifs d'e-mails non-sollicités ou de permettre à des tiers de le faire en leur fournissant les adresses recueillies ;

**2.2** Les Clients ayant souscrit des services de transit IP, d'accès Internet dédié et de colocalisation Global Crossing et fournissant ces services à leurs propres utilisateurs doivent communiquer la présente Politique d'Usages Autorisés à leurs utilisateurs sous forme de documents contractuels spécifiques et prendre des mesures pour garantir son respect par ces utilisateurs, incluant notamment la résiliation des comptes des contrevenants. Les Clients de services de transit IP, d'accès Internet dédié ou de colocalisation Global Crossing qui fournissent ces services à leurs propres utilisateurs doivent également disposer d'adresses destinées à l'envoi des notifications d'utilisations abusives pour leurs domaines, se conformer à tous les documents RFC Internet applicables, maintenir des données DNS inversées pour tous les sites hôtes connectés par le biais du réseau de Global Crossing et dont la responsabilité DNS a été déléguée au Client, maintenir des informations de contact exactes dans le registre InterNIC et autres registres de noms de domaine, IP et AS, prendre des mesures raisonnables pour empêcher les pratiques d'usurpation IP par leurs utilisateurs et clients, fournir à Global Crossing l'adresse d'un contact disponible 24 heures sur 24, 7 jours sur 7 et responsable des problèmes de sécurité et d'utilisation non-autorisée et s'assurer que les utilisateurs se conforment à la Politique d'Usages Autorisés de Global Crossing. Les mesures raisonnables à mettre en œuvre incluent notamment l'utilisation de systèmes IP « uRPF » (« unicast reverse-path forwarding ») et de mécanismes de filtrage des adresses IP lorsque cela est approprié.

### 2.3 Dispositions générales relatives aux e-mails

Il est interdit :

- d'envoyer des e-mails constitutifs de harcèlement, que ce soit par les termes utilisés, par la fréquence d'envoi ou par la taille des messages ; de continuer à envoyer des e-mails à une personne ayant sollicité l'arrêt de ces envois au motif qu'ils seraient constitutifs de harcèlement ;
- d'envoyer des e-mails perturbants (pratiques de « mail bombing » ou « bombarderie », de « flashing », etc.) ;
- d'émettre des e-mails comportant des informations d'en-tête falsifiées ;
- d'émettre des e-mails comportant des informations falsifiées ou rendues incompréhensibles (par exemple, URL codées ou masquées) pour rendre difficilement identifiable l'emplacement de l'objet de la publicité ;
- d'émettre des e-mails de type « chaîne de courriels », « système pyramidal » ou canular ;
- d'utiliser le compte de Global Crossing ou du Client pour recueillir des réponses à des messages adressés par un autre prestataire en violation des présentes règles ou de celles de cet autre prestataire ; et
- d'utiliser les services Global Crossing dans le cadre ou aux fins de l'exploitation d'un serveur de messagerie en Chine sans disposer de licence appropriée pour exploiter ce serveur.

### 2.4 Envois massifs d'e-mails :

Les Clients qui procèdent à des envois massifs d'e-mails à l'aide des services Global Crossing ne sont autorisés à le faire qu'à condition d'utiliser des « listes d'inscription en boucle fermée ». Ces Clients doivent disposer d'une méthode de confirmation ou de vérification des inscriptions et être en mesure de produire une preuve d'inscription pour les utilisateurs se plaignant de recevoir des e-mails non-sollicités. L'envoi massif d'e-mails non-sollicités (c'est-à-dire à des utilisateurs « désinscrits » ou « opt-out ») est interdit et constituera un motif de résiliation des services pour les Clients recourant à de telles pratiques. Il est interdit d'envoyer des e-mails de masse « opt-out » à partir d'un autre prestataire, encourageant ou impliquant, directement ou indirectement, l'utilisation d'un service hébergé ou fourni par Global Crossing tels que notamment des services de messagerie électronique, services Web, FTP et DNS. Les Clients s'interdisent de s'adonner à toute publicité, distribution ou utilisation de logiciels destinés à faciliter l'envoi d'e-mails « opt-out » ou à collecter à cette fin des adresses e-mails sur Internet. Les Clients s'interdisent également de vendre ou distribuer des listes d'adresses e-mail collectées dans le but d'envoyer des messages « opt-out ». Les Clients fournissant ou utilisant un service faisant appel à des identifiants de référence (« Referral ID ») seront tenus responsables des envois massifs d'e-mails non-sollicités émanant des membres du service référençant les services hébergés par Global Crossing. Les Clients recourant à des pratiques d'envoi massif d'e-mails non-sollicités, tel que décrit ci-dessus, à partir de comptes Global Crossing prendront à leur charge les coûts de main d'œuvre engagés pour traiter les réclamations, dont le montant minimum est fixé à 200 \$. Les Clients figurant sur une liste d'émetteurs de spam reconnus seront réputés enfreindre la présente Politique.

### 2.5 Newsgroups Usenet :

Les Clients doivent s'informer des travaux du réseau Usenet en consultant les questions fréquemment posées (« FAQ ») sur <http://www.faqs.org/usenet/> avant de procéder à leur inscription effective. Les éléments mis en ligne par les Clients sur les newsgroups sont soumis aux restrictions Global Crossing visées ci-dessous :

- Interdiction d'afficher des contenus illégaux, tels que montages pyramidaux/ « Ponzi », œuvres contrefaisantes ou contenus pornographiques mettant en scène des enfants ;
- Obligation de respecter les conventions et politiques ainsi que la culture spécifique de chaque newsgroup et du réseau Usenet dans son ensemble ;
- Interdiction de mettre en ligne des publicités commerciales, considérées comme inappropriées et/ou contraires au code de conduite dans la plupart des newsgroups du réseau Usenet. Des informations relatives à la publicité sur le réseau Usenet sont disponibles dans les FAQ sur la publicité sur Usenet (« Advertising on Usenet FAQ ») de Joel Furr sur [www.faqs.org/faqs/usenet/advertising/how-to/part1/](http://www.faqs.org/faqs/usenet/advertising/how-to/part1/). Pour de plus amples informations sur les courriers « spam », reportez-vous aux FAQ sur les « Limites et politiques en vigueur concernant le spam sur Usenet » sur [www.faqs.org/faqs/usenet/spam-faq/](http://www.faqs.org/faqs/usenet/spam-faq/), régulièrement mises à jour par Chris Lewis sur le newsgroup [news.admin.net-abuse.misc](mailto:news.admin.net-abuse.misc), ou consultez la page [spam.abuse.net/](http://spam.abuse.net/) ;
- Interdiction d'afficher 20 exemplaires ou plus du même article dans une période de 45 jours (pratique dite

de « spamming ») ou d'afficher de manière continue des articles non-pertinents après avoir reçu un avertissement. Les Clients ayant recours à cette pratique de « spamming » à partir de comptes Global Crossing prendront à leur charge les coûts de main-d'œuvre engagés pour procéder aux annulations et traiter les réclamations, dont le montant minimum est fixé à 200 \$. Toute pratique de spamming à partir d'un autre fournisseur encourageant ou impliquant, directement ou indirectement, l'utilisation de services hébergés ou fournis par Global Crossing tels que services de messagerie électronique, services Web, services FTP et DNS sera interdite et constituera un motif de résiliation des services pour les utilisateurs concernés ;

- Interdiction de procéder à des affichages transversaux excessifs (Indice Breidbart égal ou supérieur à 20 par période de 45 jours). L'Indice Breidbart (IB) est égal à la somme des racines carrées du nombre de newsgroups sur lesquels chaque exemplaire d'un même article est affiché. Si deux articles sont affichés, l'un sur 9 newsgroups et l'autre sur 16 newsgroups, l'indice  $IB = \text{racine carrée}(9) + \text{racine carrée}(16) = 3 + 4 = 7$ . L'affichage transversal sur des newsgroups d'articles non-pertinents est interdit ; en règle générale, l'affichage transversal d'un article sur plus de cinq newsgroups a de bonnes chances d'être non-pertinent sur au moins l'un d'entre eux ; et
- Interdiction d'afficher des articles comportant des informations d'en-tête falsifiées ; Le « travestissement » (« Munging ») d'informations d'en-tête afin de décourager la collecte d'adresses e-mail par les émetteurs de spam est toléré, à condition que des moyens raisonnables soient donnés pour répondre à l'émetteur du message. Les services de courriels anonymes peuvent être utilisés tant que cette utilisation ne viole pas la présente Politique d'Usages Autorisés d'une autre manière.

Les Clients ne peuvent émettre des annulations qu'à l'égard de leurs propres affichages, de ceux comportant un en-tête falsifié visant à créer l'illusion qu'ils ont été émis par eux et de ceux effectués dans les newsgroups dont ils assurent l'animation officielle.

## **2.6 Espace Internet et FTP :**

L'espace Internet et l'espace public FTP inclus dans un compte d'accès Internet par connexion téléphonique ne peuvent être revendus ni utilisés à des fins de transmission de contenus pour adultes. Global Crossing se réserve le droit d'exiger que les sites qui utilisent un espace Internet ou FTP bénéficiant d'un fort taux de visites soient transférés sur d'autres serveurs. Les pages Web et fichiers FTP ne peuvent contenir de documents texte ou image – qu'il s'agisse de documents hébergés sur les serveurs Global Crossing ou d'images d'un autre site affichées sur la page (« transclusion ») – violant ou enfreignant des droits d'auteur, marques, brevets, réglementations, dispositions de droit commun ou droits de propriété de tiers. Les pages Web et fichiers FTP ne peuvent contenir de liens entraînant le téléchargement de contenus contrefaisants ou autrement contraires à la loi.

## **2.7 Protocoles de routage et échange de tracés :**

Global Crossing se réserve le droit, s'il détermine que le Client envoie un nombre excessif ou superflu de publications de tracé, de limiter le nombre de tracés qui seront acceptés.

## **2.8 IRC (Internet Relay Chat) :**

L'utilisation de robots IRC est interdite, de même que les pratiques d'« inondation » (« Flooding »), de « clonage », d'usurpation, de harcèlement ou toutes autres techniques visant à entraver l'utilisation par des tiers d'espaces IRC. L'usurpation de l'identité d'autres utilisateurs, la publicité et l'envoi de spam sont également proscrits au sein des services IRC. Il est interdit d'utiliser les services IRC comme des outils de contrôle et de commande de robots. Tout Client contrevenant aux interdictions visées ci-dessus fera l'objet d'une mesure de filtrage et de blocage de la part de Global Crossing dans les 24 heures après que Global Crossing aura été informé de l'infraction. Dans un tel cas, Global Crossing n'aura aucune obligation de notification préalable à l'égard du Client.

## **2.9 Serveurs et Proxies :**

Les Clients ne sont pas autorisés à exécuter sur les serveurs Global Crossing des programmes permettant d'offrir un service ou une ressource à d'autres, tels que notamment redirecteurs de ports, serveurs de proxy, serveurs de « chat », « MUD », serveurs de fichiers et robots IRC. Par ailleurs, les Clients ne sont pas autorisés à exécuter de tels programmes sur leurs propres machines connectées par un compte d'accès Internet par connexion téléphonique Global Crossing pour offrir lesdits services ou ressources à d'autres personnes ; ils doivent disposer d'un compte d'accès dédié à cette activité. Les Clients assument l'entière responsabilité de la sécurité de leurs propres réseaux et

machines. Global Crossing décline toute responsabilité en cas de manquements ou d'atteintes aux mesures de protection implicitement ou expressément requises par le Client. Les pratiques frauduleuses résultant d'une faille de sécurité sur le système ou le compte du Client pourront entraîner la suspension par Global Crossing de l'accès aux services ou au compte ; ceci s'applique par exemple au cas où un système ferait l'objet d'une utilisation illégitime après avoir été infecté par un ver ou un cheval de Troie introduit à l'occasion d'un téléchargement Internet ou de l'exécution d'une pièce jointe à un e-mail. (Voir [www.microsoft.com/security/articles/virus101.asp](http://www.microsoft.com/security/articles/virus101.asp)) Les programmes, scripts et processus générant une charge excessive sur les serveurs Global Crossing sont interdits et Global Crossing se réserve le droit de résilier ou de suspendre un tel programme, script ou processus.

### **2.10 Connexions téléphoniques :**

Les Clients ne peuvent exécuter des programmes ou configurer des machines de telle sorte qu'une connexion téléphonique active soit maintenue lorsqu'elle n'est pas utilisée ou que la déconnexion automatique soit désactivée, sauf s'ils disposent d'un compte d'accès Internet dédié. Les Clients ne peuvent bénéficier de connexions simultanées multiples au titre d'un compte de connexion téléphonique unique. Global Crossing se réserve le droit d'imposer des restrictions aux comptes qu'il estimera contrevenir aux présentes dispositions ou de résilier lesdits comptes. Les serveurs d'accès par connexion téléphonique de Global Crossing opéreront une déconnexion au bout de 30 minutes d'inactivité et au bout de 12 heures d'accès ininterrompu.

### **2.11 Stockage de fichiers :**

Il est interdit de stocker sur les serveurs de Global Crossing des programmes, utilitaires ou fichiers dont l'utilisation constituerait une violation de la présente Politique d'Usages Autorisés. Ceci inclut par exemple le stockage de scripts pirates, de robots IRC ou de programmes de spam.

## **3. Violations et informations de contact**

**3.1 Violations :** Global Crossing déterminera à sa seule appréciation si les activités d'un Client ou son utilisation des services Global Crossing constituent une violation de la présente Politique. Global Crossing se réserve le droit de suspendre ou de résilier la fourniture d'un ou de plusieurs services Global Crossing en cas de violation ou de manquement du Client aux présentes dispositions, laquelle suspension ou résiliation (i) pourra être immédiatement effective et (ii) pourra être décidée pour une période déterminée ou non. Avant de prendre une telle mesure, Global Crossing devra en informer le Client par écrit et lui donner une opportunité raisonnable de remédier audit manquement, étant entendu, cependant, que ce délai de préavis ou de correction ne sera pas requis lorsque le manquement représente, à l'appréciation raisonnable de Global Crossing, une menace immédiate et substantielle pour l'intégrité ou la sécurité du Réseau Global Crossing ou pour les services fournis par Global Crossing aux autres utilisateurs de son Réseau. Dans un tel cas, Global Crossing notifiera au Client la suspension du service à la date de suspension effective ou après celle-ci, dès que cela est raisonnablement possible. Global Crossing s'engage à faire en sorte que l'ampleur et la durée d'une suspension de service effectuée conformément à la présente clause soient réduites à hauteur de ce que Global Crossing estime raisonnablement nécessaire pour protéger son Réseau, ses droits, sa propriété, son personnel et ses autres clients.

**3.2 Exactitude des informations :** la présente Politique est susceptible d'être modifiée moyennant notification affichée sur ce site Web. Il appartient aux Clients de surveiller sur le site Web les éventuelles modifications. La date de dernière mise à jour de la présente Politique est le 1<sup>er</sup> août 2006. Bien que s'efforçant de fournir des informations exactes et à jour sur ce site Web, Global Crossing ne fait aucune déclaration et ne consent aucune garantie concernant leur exactitude. D'autre part, des informations exactes au moment où elles sont mises en ligne peuvent devenir ultérieurement inexactes ou inapplicables. Global Crossing n'est nullement tenu de mettre à jour ces informations.

**3.3 Pour nous contacter :** veuillez adresser vos questions et commentaires concernant cette Politique par e-mail à [feedback@globalcrossing.com](mailto:feedback@globalcrossing.com). Les infractions à la présente Politique doivent être notifiées par e-mail à [abuse@gblx.net](mailto:abuse@gblx.net)