POLITIQUE INFORMATIQUE DE PERENCO

1. INTRODUCTION

Les ordinateurs et les systèmes informatiques de l'entreprise, comprenant les systèmes de messagerie et Internet, sont un composant vital de son activité et ne doivent être utilisés que par les personnes autorisées à le faire dans le cadre de l'activité de l'entreprise. Toutes les informations stockées sur les ordinateurs et systèmes de l'entreprise sont juridiquement considérées comme une propriété de l'entreprise.

1.1 Domaine d'application de cette politique

L'ensemble des employés, cadres, consultants, sous-traitants, bénévoles, stagiaires, travailleurs occasionnels, travailleurs intérimaires et toute personne ayant accès à nos systèmes informatiques et de communication (l'ensemble de ces personnes étant appelés « **employés** » dans cette politique par souci de simplicité) doivent en toute circonstance respecter cette politique informatique. Celle-ci s'applique notamment dans tous les points de présence PERENCO, notamment les bureaux des Sièges européens de Londres et de Paris, toutes les filiales, toutes les bases ainsi que leurs sites.

1.2 Conséquence d'un manquement à cette politique

Tout manquement à cette politique peut entraîner des mesures disciplinaires et, dans les cas les plus importants, peut être considéré comme une faute grave entraînant un renvoi immédiat. Toute personne qui n'est pas certaine qu'une action qu'il envisage de faire n'enfreint pas ces règles doit demander conseil à son responsable hiérarchique direct, au service informatique ou au service des relations humaines.

Les employés doivent être conscients du fait que l'entreprise peut être légalement tenue responsable de leurs manquements à cette politique et, en conséquence, l'entreprise pourra prendre toutes les mesures appropriées, y compris le signalement de toute conduite illégale aux autorités, afin de se protéger et de protéger ses filiales et son personnel. Dans un tel cas, l'entreprise sera en droit de divulguer les faits à son conseil juridique externe.

1.3 Statut juridique de cette politique

Cette politique ne fait pas partie du contrat de travail des employés et la société se réserve le droit de pouvoir la modifier à tout moment.

La direction informatique de Perenco est globalement responsable de la mise en œuvre effective de cette politique et doit assurer sa conformité au cadre légal en vigueur. La

responsabilité de la mise en œuvre de la politique au quotidien ainsi que sa maintenance et sa révision ont été déléguées au directeur informatique de Perenco.

Les employés, et plus particulièrement les cadres, ont la responsabilité de porter assistance à leurs collègues dans l'application de cette politique.

Le service informatique traitera les demandes d'autorisation ou d'assistance conformément aux dispositions de cette politique, et pourra spécifier certains standards d'équipement ou de procédures pour assurer la sécurité et la compatibilité.

1.4 Exigences de base

Afin de protéger le système :

- toute introduction de logiciel ou de matériel (PC, stockage externe, borne WiFi, etc) sur un système informatique sans autorisation est interdite,
- toute tentative d'accès non autorisé ou d'intrusion dans une partie quelconque d'un système, d'un logiciel ou d'une installation informatique sans autorisation est considérée comme une faute grave,
- vous devez respecter toutes les instructions de l'entreprise qui ont pour but de protéger les systèmes contre les virus et les logiciels malveillants (« malware »),
- vous ne devez jamais divulguer votre mot de passe à qui que ce soit,
- toute divulgation de mot de passe (dans un ticket informatique, par exemple) entraînera sa réinitialisation (ou son effacement de ses références dans un ticket par exemple) par le service informatique,
- votre poste de travail doit être verrouillé par mot de passe lorsque vous quittez votre bureau,
- vous devez éteindre votre ordinateur et votre écran lorsque vous quittez votre bureau en fin de journée.

2. SECURITE DU MATERIEL ET DES COMPTES

Les employés sont responsables de toute utilisation d'un ordinateur sous leur nom d'utilisateur et leur mot de passe, et de la sécurité du matériel qu'ils utilisent ou qui leur a été affecté. Les employés ne doivent autoriser l'utilisation de matériel ou de leurs comptes informatiques par d'autres personnes que dans le cadre de cette politique.

Pour cette raison, les employés ne doivent jamais divulguer leurs mots de passe, ni laisser des systèmes sans surveillance lorsqu'ils sont connectés aux ressources de l'entreprise. Il

relève de la responsabilité de l'employé d'informer le service informatique s'il suspecte qu'une autre personne accède à son compte.

Les employés doivent éviter de choisir des mots de passe facilement identifiables, par exemple l'utilisation de leur nom d'utilisateur dans le mot de passe, le nom de leur conjoint, de leurs animaux domestiques, de leurs enfants, des noms de famille ou des mots de passe en lien avec leurs loisirs connus. Il leur est recommandé d'éviter d'utiliser des mots du dictionnaire et d'utiliser au moins un caractère numérique et un caractère spécial dans leurs mots de passe.

Les nouveaux comptes d'employés seront créés uniquement après notification des ressources humaines ou du responsable hiérarchique par l'intermédiaire du système d'assistance intranet.

3. RESEAU ET RESSOURCES INFORMATIQUES

3.1 Responsabilités des employés

Il est interdit aux employés de rechercher, lire, copier, modifier ou supprimer les fichiers informatiques d'une autre personne sans son autorisation. Toute modification ou tentative de modification de fichiers ou systèmes sans autorisation est interdite. Toute violation intentionnelle ou fortuite de la confidentialité et de la sécurité des informations électroniques est interdite. Perenco interdit la divulgation publique non autorisée d'informations confidentielles.

Il est interdit d'interférer ou de perturber les ordinateurs ou les comptes, services ou matériel réseau d'autres employés. La propagation intentionnelle de logiciels malveillants et de virus, l'envoi de chaînes de lettres électronique (« chain mail »), les attaques par déni de service, et la diffusion inappropriée de messages à des individus ou des hôtes sont interdits.

L'analyse non autorisée de réseaux ou de ports pour rechercher des failles de sécurité est interdite.

Les connexions informatiques non autorisées sont interdites. Il est interdit d'autoriser une personne extérieure (consultant, sous-traitant, visiteur, tiers) à connecter son matériel sur le réseau de l'entreprise. Il est de la responsabilité de chaque employé de Perenco de maintenir un niveau élevé de sécurité. Le cas échéant, les consultants doivent utiliser le réseau Wi-Fi « Invité ».

Si le réseau Wi-Fi invité n'est pas disponible, un ordinateur Perenco doit être demandé avec un accès temporaire. Si des personnes extérieures doivent travailler sur site, la

préparation de leur matériel informatique peut nécessiter plusieurs jours de préparation : anticipez vos besoins.

Exceptionnellement, si des personnes extérieures doivent travailler avec leur propre ordinateur, un contrôle formel doit être effectué par le service informatique local afin de s'assurer que leur système et leur antivirus sont à jour et de vérifier que l'ordinateur externe est protégé contre les cyberattaques.

3.2 Données stockées sur le réseau

Les systèmes informatiques et le réseau informatique de l'entreprise sont exclusivement destinés à une utilisation professionnelle et toutes les données stockées sur le système sont la propriété de l'entreprise.

Les données doivent être stockées dans le dossier approprié d'un répertoire réseau partagé. Si un employé utilise les ressources de l'entreprise de manière inappropriée, il recevra une notification et il lui sera demandé d'arrêter toute activité non autorisée.

L'accès à un lecteur réseau sera accordé après l'approbation du responsable des ressources partagées par l'intermédiaire du système d'assistance informatique.

Les utilisateurs doivent être informés que seules les données enregistrées sur le réseau sont sauvegardées. Les utilisateurs d'ordinateurs portables doivent penser à copier régulièrement leurs données sur le réseau (cela s'applique également aux personnes utilisant les disques locaux de leur ordinateur). L'entreprise applique une politique de sauvegarde comprenant la conservation des sauvegardes sur bande pendant une durée de deux mois.

Les dossiers réseau partagés sont accessibles par des groupes d'utilisateurs. Ces dossiers doivent être utilisés exclusivement à des fins professionnelles et pour le stockage d'informations professionnelles uniquement.

L'importation et la rétention de données sur les systèmes de l'entreprise doivent être conformes aux clauses et conditions définies par le fournisseur des données. La conservation de données liées à un emploi précédent d'un utilisateur n'est pas autorisée sur les systèmes de l'entreprise.

Il est demandé aux employés de supprimer du réseau les données sans rapport avec l'activité de l'entreprise dans les meilleurs délais. Tout manquement entraînera la suppression et la destruction des données par le service informatique.

3.3 Services de « cloud »

L'échange de données d'entreprise au moyen de ressources de stockage sur Internet (stockage en ligne ou « cloud ») est interdit. Perenco fournit un service ftp sécurisé qui permet aux utilisateurs d'échanger des fichiers en interne comme en externe et avec des tiers.

Toute autre utilisation du « cloud » au sein de l'entreprise doit être approuvée par la direction informatique.

3.4 Infrastructure

Dans la mesure du possible, les systèmes sont protégés contre les coupures d'alimentation par un système d'alimentation sans interruption (onduleur). En cas de coupure d'alimentation, l'onduleur fournira de l'électricité pendant un temps suffisant pour permettre la mise à l'arrêt des systèmes de manière appropriée. Après une coupure d'alimentation, les systèmes critiques resteront à l'arrêt jusqu'à ce que l'autonomie totale de la batterie soit restaurée.

3.5 Confidentialité, protection des données et droits d'auteur

Toutes les données de l'entreprise sont considérées comme étant confidentielles et peuvent être soumises aux lois et règlements relatifs à la protection des données et aux droits d'auteur. Les données commercialement sensibles ne doivent en aucune circonstance être envoyées à qui que ce soit et par un quelconque moyen sans approbation ou autorisation appropriée.

4. LOGICIELS

Les logiciels piratés constituent une violation de la politique d'utilisation des logiciels. Un logiciel piraté est un logiciel qui est utilisé en violation du contrat de licence du fabricant.

Toutes les demandes d'installation d'un logiciel qui a été précédemment approuvé par le service informatique pour utilisation au sein de Perenco doivent être transmises par l'intermédiaire du système d'assistance informatique. Les applications non encore approuvées doivent être préalablement contrôlées par la direction informatique avant toute installation.

Perenco s'efforce d'assurer la cohérence de ses standards de logiciels. Pour cette raison, l'utilisation de logiciels non standard et/ou personnels doit rester limitée. L'installation d'un logiciel personnel nécessite l'approbation préalable de votre responsable hiérarchique direct et du service informatique. Une preuve de propriété (telle qu'une copie de la licence)

doit être fournie au service informatique, en cas d'audit de logiciels. L'utilisation de logiciels contributifs (« shareware ») et gratuits (« freeware ») entre dans le cadre de cette politique. Tous les logiciels non autorisés trouvés sur un système informatique seront immédiatement supprimés.

Les applications développées par un utilisateur (Access, macros Excel, etc.) relèvent de la responsabilité de leur auteur et ne bénéficieront pas du support du personnel des services informatiques Perenco. L'auteur est responsable de toute mise à niveau ou correction de défaut de telles applications. Seules les applications développées en collaboration avec le service informatique de Perenco bénéficient de son support.

Les employés ne sont pas autorisés à utiliser les ressources informatiques de Perenco pour concevoir, créer ou propager des programmes informatiques malveillants.

Perenco se réserve le droit de réclamer à un employé tout paiement ou compensation que l'entreprise serait amenée à payer à des tiers consécutivement à une violation par l'employé des politiques ci-dessus.

5. COURRIEL

La taille des boîtes de messagerie est limitée. Si la boîte de messagerie d'un employé dépasse cette limite, il recevra automatiquement un courriel l'informant du problème. Si l'employé ne réduit pas la taille de sa boîte de messagerie, il pourrait être incapable d'envoyer ou de recevoir des courriels jusqu'à ce que la boîte atteigne une taille appropriée.

Cette politique s'applique à tous les comptes de messagerie personnels utilisés pour communiquer des données liées à l'entreprise.

Les messages échangés par courriel peuvent être divulgués dans le cadre de procédures judiciaires de la même façon que des documents sur papier. La suppression de messages de la boîte de réception ou des archives d'un utilisateur ne signifie pas qu'il n'est plus possible de récupérer un courriel à des fins de divulgation. Tous les courriels doivent être traités comme étant potentiellement consultables, sur le serveur principal ou en utilisant un logiciel spécialisé.

5.1 Utilisation générale des courriels

L'utilisation du système de messagerie de l'entreprise pour envoyer ou transférer des messages au contenu diffamatoire, insultant, discriminatoire, sexuellement explicite,

calomnieux et illégal, qui constituent un harcèlement sexuel ou qui sont autrement inappropriés est interdite. De même, si un employé reçoit un courriel obscène ou diffamatoire, de façon involontaire ou autre depuis une source quelconque, il doit le supprimer et ne pas le transférer à une autre adresse sauf si l'employé souhaite déposer une plainte officielle contre l'envoyeur dans le cadre de la politique disciplinaire de l'entreprise. Il doit alors contacter son responsable hiérarchique ou le service des ressources humaines. La politique de Perenco interdit la falsification d'une adresse électronique et/ou l'inclusion de fausses informations dans l'en-tête du courriel. Il est illégal d'usurper l'identité d'un autre employé par courriel.

Les employés doivent être attentifs au contenu des messages échangés par courriel, car des déclarations incorrectes ou inappropriées peuvent entraîner des plaintes pour discrimination, harcèlement, diffamation, violation de confidentialité ou violation de contrat. Les employés doivent partir du principe que tous les courriels peuvent être lus par d'autres personnes et ne doivent inclure aucun contenu susceptible d'offenser ou d'incommoder les lecteurs, ou eux-mêmes, si celui-ci était divulgué dans le domaine public.

5.2 Archivage des courriels

Perenco dispose un outil d'archivage automatique des courriels pour gérer le volume sans cesse croissant de messages et essaie de le mettre en place sur tous ses sites. Par conséquent, partout où ce système est disponible, l'utilisation de fichiers de « dossiers personnels Outlook » (.pst) n'est pas supportée.

6. POLITIQUE D'UTILISATION D'INTERNET

Les fichiers téléchargés sur Internet doivent être analysés pour y rechercher d'éventuels virus. Il est interdit de télécharger des fichiers comportant du contenu offensant.

Lorsqu'un employé visite un site Internet, des dispositifs tels que des cookies, des tags ou des balises web peuvent être utilisées pour permettre au propriétaire du site d'identifier et de surveiller des visiteurs. Si le site Internet est de type inapproprié ou restreint, un tel marqueur peut être une source d'embarras pour le visiteur et pour l'entreprise, en particulier en cas d'accès, téléchargement, stockage ou transfert de contenu inapproprié depuis le site Internet. Dans certains cas, de telles actions peuvent constituer un délit si, par exemple, le contenu est de nature pornographique.

6.1 Restriction de sites Internet

Les employés ne doivent pas accéder à une page Web ou télécharger une image, un document ou un autre fichier sur Internet qui pourrait être considéré comme illégal ou offensant.

Afin d'autoriser l'accès aux sites Internet légitimes et désactiver l'accès aux sites Internet qui sont jugés inappropriés ou présentant un risque de sécurité, l'entreprise a installé un logiciel de restriction de sites Internet qui désactive l'accès au site de catégories ou types particuliers.

Le comité directeur informatique a établi une liste de ces catégories de sites Internet qui sont considérés comme non professionnels. Ces catégories seront inaccessibles dans toutes les filiales de Perenco. La direction locale a le droit d'imposer une restriction d'accès à Internet plus stricte. L'utilisateur est pleinement responsable des visites de sites Internet ou téléchargements de données.

6.2 Réseaux sociaux

En règle générale, depuis les réseaux de l'entreprise, l'accès aux sites Internet de réseaux sociaux à des fins non professionnelles n'est pas autorisé. Suivant la politique de la direction locale, cet accès peut être interdit.

L'entreprise respecte le droit d'un employé à avoir une vie privée. Cependant, elle doit également s'assurer que la confidentialité et sa réputation sont protégées. Par conséquent, elle exige de ses employés utilisant des sites de réseaux sociaux qu'ils veillent à :

- ne pas avoir une conduite susceptible de nuire à l'entreprise, ses filiales et ses employés,
- éviter que leur interaction sur ces sites nuise aux relations professionnelles entre les membres du personnel et les clients de l'entreprise,
- ne transmettre aucune information pouvant donner à une personne un accès non autorisé aux informations de l'entreprise et/ou toute information confidentielle,
- n'enregistrer aucune information relative à l'entreprise sur les réseaux sociaux, tels que sa structure, les technologies utilisées ou ses réseaux.

7. ACCES A DISTANCE

Le service d'accès à distance permet aux employés d'accéder à des services depuis l'extérieur du réseau de façon sécurisée.

L'autorisation d'accès est approuvée par le responsable hiérarchique de l'employé. Le processus et les fichiers de configuration d'accès à distance sont destinés à être utilisés exclusivement par l'employé et ne doivent pas être divulgués à un tiers.

Chaque responsable hiérarchique recevra une notification hebdomadaire des accès dont il est responsable. L'accord ou la suppression d'un droit d'accès distant à un employé, un sous-traitant ou un tiers relève de la responsabilité de leurs responsables hiérarchiques. Tous les employés se connectant au réseau à distance doivent se conformer à la politique informatique.

Tous les employés ayant un droit d'accès à distance doivent être référencés dans la base de données du personnel de l'intranet afin de tenir à jour les références exactes des employés et le nom de leur responsable hiérarchique.

Le cas échéant, l'entreprise se réserve le droit de déconnecter ou supprimer des comptes d'accès à distance, par exemple, en cas de violation de sécurité.

8. APPAREILS PORTABLES

La politique informatique s'applique également à tous les employés à qui un appareil portable appartenant à l'entreprise a été affecté, tels que des ordinateurs portables, des smartphones et des périphériques de stockage externe.

Les employés doivent garder à l'esprit que les appareils portables contiennent des données de l'entreprise (dont certaines peuvent être des données personnelles protégées par les lois relatives à la protection des données). Les employés doivent veiller à conserver ces appareils portables en lieu sûr, en particulier lors de déplacements, et ils doivent prendre toutes les mesures appropriées pour les protéger en toute circonstance contre une utilisation non autorisée, une perte ou un vol.

Toute perte d'un appareil portable de l'entreprise doit être signalée au service informatique dans les plus brefs délais afin qu'il puisse être désactivé. Cela s'applique également aux appareils endommagés.

Comme pour toute propriété de l'entreprise, les appareils portables doivent être retournés cette dernière lorsque l'employé la quitte. Tout manquement entraînera automatiquement la déduction du coût d'un appareil de remplacement du solde final de l'employé.

L'entreprise se réserve le droit d'accéder à distance ou de désactiver tout appareil portable se connectant au réseau de l'entreprise sans autorisation.

9. USAGE PERSONNEL

La Société autorise l'utilisation occasionnelle des systèmes Internet, de messagerie et téléphoniques de l'entreprise pour envoyer des courriels personnels, naviguer sur Internet et passer des appels téléphoniques personnels dans le respect de certaines conditions décrites ci-dessous. L'utilisation personnelle est un privilège et non un droit. Il ne doit pas faire l'objet d'une utilisation excessive ou d'abus. Cette autorisation peut être retirée ou sa portée limitée, à tout moment, à la discrétion du Management de la société.

L'utilisation personnelle est soumise aux conditions suivantes :

- l'utilisation doit être réduite au minimum,
- les courriels personnels doivent comporter la mention « personnel » dans l'en-tête du sujet,
- l'utilisation ne doit pas interférer avec les activités professionnelles,
- l'utilisation ne doit entraîner qu'un coût marginal pour l'entreprise,
- l'utilisation doit être conforme aux politiques de l'entreprise (telles que celles concernant l'égalité de traitement, le harcèlement, la protection des données et les procédures disciplinaires).

La Société se réserve le droit de restreindre ou d'interdire l'accès à certains numéros de téléphone ou sites Internet si elle considère que l'utilisation personnelle en est excessive.

10. SURVEILLANCE

Si nécessaire, les systèmes de la société permettraient de surveiller les communications téléphoniques, les courriels, messageries vocales, et les communications sur Internet et autres. Afin de protéger l'entreprise et de remplir ses obligations légales en tant qu'employeur, l'utilisation des systèmes, comprenant les systèmes téléphoniques informatiques, et toute utilisation personnelle de ceux-ci, peut être surveillée en permanence par un logiciel automatisé ou autre. Cette surveillance n'est conduite que dans le cadre défini par la loi et dans une mesure nécessaire et justifiable pour le bien de l'entreprise.

D'autre part, Perenco se réserve le droit de mettre en œuvre des systèmes de vidéosurveillance autonome dans certaines parties de nos bureaux, installations et sites, y

compris, sans s'y limiter, les espaces extérieurs, les zones de réception, les entrées et les sorties. Ces données ne sont contrôlées et enregistrées que par du personnel autorisé.

Perenco se réserve le droit de contrôler, intercepter, enregistrer et extraire des communications, comprenant le contenu de messages électroniques ou de vérifier l'utilisation d'Internet (telles que les pages visitées et les recherches effectuées), dans la limite du raisonnable et dans l'intérêt de l'entreprise, aux fins suivantes (cette liste n'étant pas exhaustive) :

- vérifier que l'utilisation du système de messagerie électronique ou d'Internet est légitime et conforme à sa politique,
- retrouver des messages perdus ou extraire des messages perdus en raison d'un défaut informatique (par exemple, si un employé est absent pour une raison quelconque, il peut être nécessaire de contrôler les communications pour assurer le bon fonctionnement de l'entreprise),
- contribuer à l'investigation d'une faute présumée (par exemple, si l'entreprise suspecte un employé d'envoyer ou de recevoir des courriels qui nuisent à l'entreprise, ses filiales ou ses employés),
- se conformer à des obligations légales éventuelles,
- établir l'existence de faits relatifs à l'entreprise (par exemple si l'entreprise suspecte que l'employé a passé un temps excessif à consulter des sites Internet qui ne sont pas liés à son activité professionnelle),
- établir la conformité à des pratiques ou procédures réglementaires relatives à la conduite de l'activité de l'entreprise (par exemple, si l'entreprise suspecte qu'un employé a consulté du contenu offensant ou illégal),
- établir ou démontrer le respect de standards par des personnes utilisant le système dans le cadre de leur mission professionnelle,
- prévenir ou détecter un crime, ou
- enquêter sur une utilisation non autorisée des systèmes, par exemple pour rechercher des virus ou d'autres menaces pour le système.

Les courriels et fichiers de données liés aux employés peuvent être archivés et conservés pendant une durée minimale de deux ans.