	<p>DECISION N° <u>536</u> /DG</p> <p>OBJET : CHARTE D'UTILISATION DU SYSTÈME D'INFORMATION DE SONATRACH</p>	<p>Classement : 0.007.5/20</p> <p>Référence : E-023 (R1)</p> <p>Page : 1 de 1</p>
---	---	---

Le Président Directeur Général,

Vu le décret présidentiel n°98-48 du 11 février 1998, modifié et complété, portant statuts de SONATRACH ;

Vu le décret présidentiel du 05 février 2020, portant nomination de Monsieur Toufik HAKKAR en qualité de Président Directeur Général de SONATRACH ;

Vu la décision A-001 (R31) du 19 juin 2018, portant organisation de la macrostructure de SONATRACH ;

Vu la décision E-023 du 04 juillet 2012, portant charte informatique des utilisateurs de SONATRACH.

DECIDE

ARTICLE 1 : La présente décision annule et remplace la décision E-023 du 04 juillet 2012, portant charte informatique des utilisateurs de SONATRACH.

ARTICLE 2 : Cette décision a pour objet de définir les règles et les principes de la charte d'utilisation du système d'information de SONATRACH. Elle détermine en son annexe, les règles d'utilisation des ressources informatiques et des services communs de la Société.

ARTICLE 3 : La présente charte s'applique à l'ensemble du personnel de la Société, permanent ou temporaire, ainsi que tout agent stagiaire, consultant, utilisant à quelque titre que ce soit, les ressources informatiques de la Société.

ARTICLE 4 : La présente charte est portée à la connaissance des utilisateurs des ressources informatiques de la Société par les moyens de diffusion interne.

ARTICLE 5 : La charte d'utilisation du système d'information de SONATRACH fera l'objet de révision selon les changements d'environnement technologique et/ou réglementaire.

ARTICLE 6 : La présente décision est complétée par l'annexe unique portant charte d'utilisation du système d'information de SONATRACH.

ARTICLE 7 : La présente décision prend effet à compter de la date de sa signature.

ARTICLE 8 : Le Secrétaire Général, le Directeur de Cabinet, les Vice-Présidents, le Directeur Exécutif, les Directeurs Centraux et les Directeurs des structures rattachées à la Direction Générale sont chargés, chacun en ce qui le concerne, de l'exécution de la présente décision.

Fait à Alger, le

11 NOV. 2020

7 Le Président Directeur Général,

T. HAKKAR





SOMMAIRE

GLOSSAIRE

ANNEXE I : CHARTE D'UTILISATION DU SYSTEME D'INFORMATION DE SONATRACH

PREAMBULE

I.1. OBJET

I.2. OBJECTIF

I.3. CHAMP D'APPLICATION

I.4. OBLIGATIONS ET RESPONSABILITES

I.4.1. OBLIGATIONS DE SONATRACH

I.4.2. OBLIGATIONS DE L'UTILISATEUR

I.4.3. RESPONSABILITES

I.4.4. CONFIDENTIALITE

I.5. COMPTE UTILISATEUR ET DROITS D'ACCES

I.6. STOCKAGE DES DONNEES

I.7. UTILISATION DES LOGICIELS

I.7.1. LOGICIELS SOUS LICENCE

I.7.2. LOGICIELS LIBRES

I.7.3. LOGICIELS DEVELOPPES EN INTERNE

I.7.4. DONNEES ET MODELES

I.8. UTILISATION DE LA MESSAGERIE ELECTRONIQUE

I.8.1. REGLES DE SECURITE

I.8.2. REGLES DE BON USAGE

I.8.3. UTILISATION DE LA MESSAGERIE A DES FINS PERSONNELLES

I.8.4. SUPERVISION DE L'UTILISATION DE LA MESSAGERIE

I.9. UTILISATION D'INTERNET

I.9.1. REGLES DE BON USAGE DE LA NAVIGATION SUR INTERNET

I.9.2. UTILISATION D'INTERNET A DES FINS PERSONNELLES

I.9.3. UTILISATION DES RESEAUX SOCIAUX

I.9.4. SUPERVISION DE LA NAVIGATION INTERNET

I.10. UTILISATION DES EQUIPEMENTS INFORMATIQUES

I.10.1. EQUIPEMENTS INFORMATIQUES MIS À DISPOSITION PAR SONATRACH


A



- I.10.2. REGLES DE SECURITE DES EQUIPEMENTS INFORMATIQUES**
- I.10.3. REGLES DE SECURITE DES EQUIPEMENTS MOBILES**
- I.10.4. RESTITUTION DES EQUIPEMENTS INFORMATIQUES**
- I.10.5. DECLARATION DE PERTE OU DE VOL D'EQUIPEMENTS MOBILES**
- I.10.6. UTILISATION D'EQUIPEMENTS INFORMATIQUES A DES FINS PERSONNELLES**
- I.10.7. EQUIPEMENTS INFORMATIQUES PERSONNELS**
- I.10.8. CONTROLE ET SUPERVISION DES EQUIPEMENTS INFORMATIQUES**
- I.11. PROTECTION CONTRE LES MALWARES**
- I.12. DONNEES PRIVEES**
- I.13. ACCES A DISTANCE VIA VPN**
- I.14. MESURES DE SECURITE LORS DES DEPLACEMENTS HORS SOCIETE**
- I.15. DROITS DE PROPRIETE INTELLECTUELLE**
- I.16. MANQUEMENT AU RESPECT DE LA CHARTE ET SANCTIONS**



GLOSSAIRE

Activité illicite	Toute utilisation ou manipulation, des ressources du système d'information mis à la disposition de l'utilisateur à des fins d'une activité contraire aux lois en vigueur ou de nature à porter atteinte à l'ordre public ou aux bonnes mœurs.
Code QR (Code Quick Response )	Désigne un type de code en deux dimensions qui peut être lu et décodé par les smartphones, les tablettes ou autres moyens. Ce code permet de stocker des informations numériques (texte, adresse web, carte de visite, ...).
Compte	Désigne l'association d'un identifiant d'Utilisateur et d'un mot de passe, constituant la clef d'accès à certaines ressources du système d'information.
Débridage	Désigne l'action de contourner les protections d'un système pour supprimer les restrictions d'utilisation mises en place par le constructeur, l'action est souvent appelée rooting ou jailbreak.
Donnée classifiée	Désigne toute donnée à protéger au sens de la procédure de classification, transmission et sécurisation de l'information en vigueur dans la Société.
Donnée privée	Désigne tout fichier stocké dans un répertoire nommé explicitement « Privé » par l'Utilisateur ou tout message électronique portant la mention « Privé » dans son objet.
Equipement informatique	Désigne tout équipement mobile, ordinateur de bureau, imprimante, copieur, Fax, scanner, moniteur (écran), serveur, téléphone (DECT inclus), modem, support amovible, équipement de visioconférence (caméra, casque, ...) et tout autre équipement informatique qui viendrait s'ajouter à cette liste dans le futur.



Equipement mobile	Désigne tout équipement informatique que l'on peut utiliser lors d'un déplacement sans nécessité de branchement électrique (laptop, netbook, notebook, tablette, smartphone, ...).
Hoax	Désigne toute information fausse relayée à grande échelle grâce à internet.
Licence	Désigne un contrat par lequel l'éditeur d'un logiciel définit les conditions de son utilisation.
Logiciel libre	Un logiciel est qualifié de libre quand ses détenteurs ont la liberté de l'exécuter, le copier, le distribuer, l'étudier, et le modifier éventuellement.
Malware	Désigne tous les programmes hostiles ou intrusifs et souvent très nuisibles au système d'information. Ils sont de différents types : virus, cheval de Troie, ver, ransomware, spyware, adware, etc.
Messagerie instantanée	Désigne toute application qui permet d'échanger des messages multimédias en temps réel entre plusieurs personnes utilisant cette application.
Plugin ou Plug-in	Désigne un petit programme qui se greffe à un logiciel pour lui conférer de nouvelles fonctionnalités, notamment sur un navigateur pour lui apporter des fonctions supplémentaires.
Poste de travail	Désigne le point d'accès, dans la Société, aux ressources du système d'information, via ordinateur de bureau ou laptop.
Recommandations de sécurité du logiciel	Désigne le guide de configuration du logiciel permettant de le déployer de manière sécurisée. Il est basé sur les principes fondamentaux en matière de sécurité des systèmes d'information.
Ressource du système d'information	Désigne tout équipement des technologies de l'information et de la communication mis à la disposition de l'utilisateur ainsi que les espaces de stockage, les logiciels, les applications et les bases de données auxquels les utilisateurs ont accès.
Structure habilitée	Désigne toute entité organique compétente, généralement la structure informatique, en charge de fournir des prestations liées au système d'information de SONATRACH.

A



Support amovible	Désigne tout support de stockage relié à un équipement informatique qui peut être retiré et transporté (carte SD, clé USB, Disque externe, CD, DVD, ...).
Système d'information	Désigne l'ensemble des ressources qui permettent de collecter, stocker, traiter et distribuer de l'information.
Technologies de l'information et de la communication	Désignent toutes les techniques de l'informatique et des télécommunications permettant aux utilisateurs d'accéder, de manipuler, de stocker, de produire et de communiquer l'information.
Utilisateur	Désigne tout agent SONATRACH disposant de droits d'accès aux ressources du système d'information et ce, quel que soit son statut et sa position. Utilisateur désigne aussi tout apprenti, stagiaire, consultant, conseiller, employé de société de prestataire ou visiteur occasionnel bénéficiant de droits d'accès aux ressources du système d'information dans le cadre de dispositions contractuelles avec SONATRACH.
VPN (Virtual Private Network)	Désigne un moyen sécurisé de communication, à distance, entre deux ordinateurs, très souvent via internet.



N° 536 /DG

Classement : 0.007.5/20

Référence : E-023 (R1)

Page : 1 de 16

ANNEXE

**CHARTRE D'UTILISATION DU SYSTEME D'INFORMATION DE
SONATRACH**



PREAMBULE

L'évolution fulgurante des technologies de l'information et de la communication, et la diversification des solutions accroissent la nécessité de reconsidérer la politique d'utilisation des ressources du système d'information de SONATRACH, notamment, à travers la révision de sa charte d'utilisation du système d'information.

Cette version de la charte s'inscrit dans cette optique et vient conforter la régulation de l'usage des ressources du système d'information de SONATRACH, bannir les abus et les fraudes informatiques et prévenir les éventuels risques pouvant impacter la performance du système d'information de la Société.

En vertu de cette charte, l'utilisateur est informé de ses droits et de ses obligations ainsi que des limites d'utilisation des ressources du système d'information mises à sa disposition. L'utilisateur s'engage à respecter les règles édictées dans la présente charte partant du principe que toutes les ressources mises à sa disposition dans un but professionnel sont la propriété exclusive de SONATRACH.

Aussi, toute utilisation contraire aux dispositions de la présente charte constitue une faute grave passible de sanction disciplinaire.

Cette charte vient en complément aux lois en vigueur que l'utilisateur est censé connaître et respecter.

I.1. OBJET

La présente charte a pour objet de définir les règles et les modalités d'utilisation des ressources du système d'information de SONATRACH mises à la disposition des utilisateurs dans le cadre de l'exercice de leurs fonctions. Elle met en évidence leurs droits et obligations ainsi que leurs responsabilités en cas de manquement au respect de la présente charte, tout en les informant des mesures de contrôle et de supervision mises en place, dans le souci de préserver la sécurité, l'intégrité et la performance du système d'information de la Société.

I.2. OBJECTIF

La présente charte vise à préserver le système d'information de SONATRACH, réglementer l'usage de ses ressources et sensibiliser les utilisateurs pour une utilisation conforme aux bonnes pratiques à même de pérenniser son intégrité face aux abus et aux cyberattaques.

I.3. CHAMP D'APPLICATION

La présente charte s'applique à tous les utilisateurs. Elle s'applique, au même titre, aux utilisateurs autorisés à accéder au système d'information de SONATRACH via leurs équipements informatiques personnels.

I.4. OBLIGATIONS ET RESPONSABILITES

I.4.1. OBLIGATIONS DE SONATRACH

SONATRACH, par le biais de ses structures, doit :

- Mettre à la disposition de l'utilisateur les ressources du système d'information nécessaires à l'exercice de ses fonctions ;



- Garantir le bon fonctionnement et la disponibilité des ressources du système d'information ;
- Mettre en œuvre les moyens nécessaires susceptibles d'assurer la confidentialité et l'intégrité des données professionnelles et des échanges électroniques ;
- Assurer une large diffusion de la présente charte et informer les utilisateurs des politiques et des procédures en la matière ;
- Informer les utilisateurs des politiques et des procédures en vigueur en matière de sécurité du système d'information ;
- Informer les utilisateurs qu'un contrôle et une supervision de l'usage des ressources du système d'information sont mis en place ;
- Veiller à la sensibilisation régulière des utilisateurs sur les risques liés à la sécurité du système d'information.

I.4.2. OBLIGATIONS DE L'UTILISATEUR

L'utilisateur doit :

- Respecter la présente charte et veiller au strict respect de son application par les utilisateurs sous sa responsabilité ;
- Concourir à la protection des ressources du système d'information mises à sa disposition dans le cadre de l'exercice de ses fonctions ;
- Signaler à la structure habilitée toute violation ou tentative de violation de l'intégrité des ressources du système d'information mises à sa disposition ;
- Ne pas modifier les paramétrages de l'équipement informatique et des ressources du système d'information mis à sa disposition, ni tenter de contourner aucun des systèmes de sécurité mis en place par SONATRACH ;
- Ne pas se livrer à une activité concurrente à celle de SONATRACH ou susceptible de lui causer un quelconque préjudice en utilisant son système d'information.

I.4.3. RESPONSABILITES

L'utilisateur est le responsable direct de l'usage des ressources du système d'information mises à sa disposition dans le cadre de l'exercice de ses fonctions. Tout manquement aux dispositions de la présente charte engage la responsabilité de l'utilisateur, en vertu du règlement intérieur et sous peine de poursuites judiciaires.

I.4.4. CONFIDENTIALITE

- L'utilisateur est tenu à l'obligation du secret professionnel et ne doit en aucun cas divulguer des données qu'il manipule dans le cadre de l'exercice de ses fonctions ;
- L'utilisateur ne doit pas tenter de prendre connaissance des données que seuls d'autres utilisateurs sont autorisés à manipuler ;
- Les utilisateurs administrateurs de ressources du système d'information ne doivent en aucun cas prendre connaissance des données et informations auxquelles ils peuvent accéder dans le cadre de l'exercice de leurs fonctions. Ils doivent respecter les règles d'éthique et de déontologie définies dans des procédures et documents spécifiques.



I.5. COMPTE UTILISATEUR ET DROITS D'ACCES

L'attribution d'un compte à un utilisateur donne lieu à des droits d'accès spécifiques aux ressources du système d'information de SONATRACH.

L'utilisateur est responsable de l'usage des ressources du système d'information sur lesquelles il dispose de droits d'accès.

L'utilisateur doit :

- Mémoriser le mot de passe de son compte et le garder strictement confidentiel ;
- Veiller à définir des mots de passe complexes et procéder régulièrement à leur changement ;
- Verrouiller sa session de travail avant de quitter son poste de travail ;
- Signaler, à la structure habilitée, toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- Signaler, à la structure habilitée, tout droit d'accès non afférent à ses fonctions (*accès à certains fichiers, affectation à un groupe, ...*) ;
- Informer la structure habilitée de tout changement de poste ou d'habilitations impliquant une modification de ses droits d'accès ou ceux de ses subordonnés.

L'utilisateur ne doit pas :

- Communiquer son compte à d'autres utilisateurs. Le compte est strictement nominatif ;
- Utiliser ou tenter d'utiliser des comptes autres que le sien ;
- Conserver le mot de passe de son compte en lieu non sûr (post-it sur le bureau, fichier en clair, etc.) ;
- Utiliser le même mot de passe pour les accès professionnels et personnels.

I.6. STOCKAGE DES DONNEES

SONATRACH met à la disposition des utilisateurs des espaces de stockage sécurisés dédiés exclusivement aux données professionnelles. SONATRACH se réserve le droit de procéder à la suppression des données non professionnelles sans préavis.

L'utilisateur doit :

- Veiller à ne stocker les données professionnelles que sur les espaces de stockage sécurisés fournis par la structure habilitée ;
- Veiller à ne pas saturer les espaces de stockage fournis par la structure habilitée par des données inutiles ;
- Se conformer aux dispositions de la procédure de sécurisation des documents électroniques classifiés en vigueur à SONATRACH lors du stockage de données classifiées ;
- Supprimer les données classifiées transportées sur des supports amovibles après leur transfert sur l'espace de stockage fourni par la structure habilitée ;
- Signaler, à la structure habilitée, la perte de données sous sa responsabilité ;
- Faire attention au risque de suppression ou de modification lors de la manipulation de données stockées sur un espace partagé.

A



L'utilisateur ne doit pas :

- Stocker sur les espaces de stockage fournis par la structure habilitée des données autres que professionnelles ;
- Stocker les données professionnelles sur des espaces de stockage externes à SONATRACH ou sur tout autre support amovible ou équipement non fourni par la Société.

I.7. UTILISATION DES LOGICIELS

I.7.1. LOGICIELS SOUS LICENCE

Toute utilisation de logiciel non conforme aux conditions définies dans sa licence est illicite. L'utilisation de licence à usage exclusivement étudiantin ou personnel sur les ressources du système d'information de la société est interdite et porte préjudice à SONATRACH. Dans les deux cas la responsabilité pénale de l'utilisateur est engagée.

L'utilisateur est responsable de l'usage des logiciels mis à sa disposition par la Société, il est tenu de faire preuve d'un usage loyal et rationnel en respectant, notamment les règles ci-après.

L'utilisateur doit :

- Signaler à la structure habilitée toute tentative de violation de licence de logiciel et, de manière générale, tout dysfonctionnement constaté de logiciel, d'application ou d'utilitaire installé sur le poste de travail ;
- Respecter les recommandations de sécurité du logiciel lors de toute manipulation de données extraites du système d'information.

L'utilisateur ne doit pas :

- Désinstaller, modifier ou empêcher la bonne exécution des logiciels installés sur son poste de travail par la structure habilitée ;
- Installer, ni télécharger des logiciels sur son poste de travail sans l'autorisation de la structure habilitée ;
- Contourner les restrictions d'utilisation d'un logiciel mis à sa disposition ;
- Réaliser des copies de logiciels, exceptées les copies de sauvegarde ;
- Mettre à la disposition de tiers des logiciels fournis par la Société.

I.7.2. LOGICIELS LIBRES

Le recours par l'utilisateur à l'usage d'un logiciel libre doit être motivé. La structure habilitée se prononce sur l'autorisation ou pas de l'usage du logiciel libre en tenant compte des paramètres de compatibilité, de sécurité, de support et d'évolutivité.

I.7.3. LOGICIELS DEVELOPPES EN INTERNE

Tout logiciel ou macro développé en interne par les moyens et le personnel de la Société est la propriété exclusive de SONATRACH. Les codes sources des logiciels développés en interne doivent être stockés sur les espaces sécurisés mis à disposition par la structure habilitée.



I.7.4. DONNEES ET MODELES

Toute donnée générée ou modèle développé en interne par les moyens et le personnel de la Société, est la propriété exclusive de SONATRACH et devraient être stockés sur les espaces sécurisés mis à disposition par la structure habilitée.

I.8. UTILISATION DE LA MESSAGERIE ELECTRONIQUE

La messagerie électronique de SONATRACH est mise à la disposition des utilisateurs pour un usage professionnel. La réception de messages provenant de domaines publics est bloquée, sauf exception de nécessité de service dûment justifiée.

L'utilisateur est tenu de préserver le bon fonctionnement du service de messagerie électronique de SONATRACH par le respect des règles de sécurité et de bon usage définies infra et s'abstenir, entre autres, de diffuser des messages, des documents, des informations, des images ou des vidéos, particulièrement :

- Portant atteinte à l'image de marque de SONATRACH ou de ses partenaires ;
- Portant atteinte au respect des droits des personnes et droits publics ;
- De publicité ou de propagande ;
- À caractère ludique, religieux ou éducatif.

I.8.1. REGLES DE SECURITE

L'utilisateur doit :

- Utiliser exclusivement la messagerie de SONATRACH lors des échanges professionnels ;
- Vérifier, avant l'envoi de messages, l'identité des destinataires et leur habilitation à recevoir les informations transmises. Cette vérification doit être renforcée pour les messages véhiculant des données classifiées ;
- Protéger les messages contenant des données classifiées conformément aux directives de la procédure de sécurisation des documents électroniques classifiés en vigueur.

L'utilisateur ne doit pas :

- Ouvrir les messages électroniques reçus de source douteuse, ces messages devront être impérativement supprimés ;
- Cliquer sur tout lien ou ouvrir des pièces jointes contenus dans des messages dont l'origine semble douteuse ;
- Tenter d'accéder à des messages autres que les siens. En cas de réception par erreur d'un message professionnel dont on n'a pas l'habilité, prévenir immédiatement l'expéditeur et procéder à la suppression du message ;
- Utiliser l'adresse email professionnelle pour l'inscription aux réseaux sociaux ou souscrire notamment, à des groupes de Newsletter ou forums non professionnels ;
- Paramétrer le transfert automatique du contenu de sa boîte de messagerie SONATRACH vers une adresse de messagerie extra SONATRACH ;
- Procéder à des diffusions de messages non professionnels pouvant entraîner la saturation et la dégradation du service de messagerie ;



- Relayer des messages de type Hoax comportant des instructions demandant de les faire suivre à d'autres personnes ;
- Envoyer des messages vers des domaines publics sauf cas de nécessité de service.

I.8.2. REGLES DE BON USAGE

L'utilisateur doit :

- Utiliser le service de messagerie électronique SONATRACH dans le respect de la voie hiérarchique ;
- Faire preuve de correction à l'égard de ses interlocuteurs dans les échanges électroniques professionnels tout en préservant l'intérêt et la réputation de la Société ;
- Éviter de ralentir le fonctionnement de la messagerie électronique par la transmission de fichiers de taille importante et favoriser plutôt l'utilisation de liens vers les fichiers sur des espaces de stockage partagés ;
- Prendre toutes les précautions nécessaires de sécurité lors de l'utilisation de la messagerie SONATRACH à distance (*via internet*), particulièrement dans les lieux publics ;
- Demander au destinataire de confirmer la réception par retour d'email et activer l'accusé de réception lors de l'envoi de messages importants pour plus de traçabilité ;
- Activer la règle de réponse automatique en cas d'absence et communiquer éventuellement les coordonnées de son remplaçant ;
- Utiliser la fonctionnalité Copie carbone invisible « Cci » de l'outil de messagerie électronique à bon escient ;
- Ne pas saturer sa boîte de messagerie et procéder régulièrement à l'archivage des messages professionnels importants (reçus et envoyés), afin de garder la traçabilité des dossiers, notamment stratégiques et veiller à ne supprimer que les messages inutiles.

I.8.3. UTILISATION DE LA MESSAGERIE A DES FINS PERSONNELLES

L'utilisation de la messagerie SONATRACH à des fins personnelles n'est tolérée qu'à titre exceptionnel et limité dès lors qu'elle ne remette pas en cause ni le bon fonctionnement du service de messagerie ni sa sécurité. Tous les messages échangés via la messagerie SONATRACH sont considérés comme documents professionnels sauf ceux comportant explicitement la mention « privé » dans leurs objets. L'utilisation à des fins personnelles reste, cependant, soumise aux mêmes règles édictées dans les points I.8., I.8.1. et I.8.2. SONATRACH n'est pas responsable de la sauvegarde ou de la sécurité des messages privés. Les utilisateurs sont appelés à user des messageries publiques pour leurs échanges personnels.

I.8.4. SUPERVISION DE L'UTILISATION DE LA MESSAGERIE

L'utilisateur est informé qu'un dispositif de filtrage, supervision et de contrôle est mis en place par la Société pour s'assurer du bon fonctionnement du service de messagerie électronique et contrôler son utilisation. L'utilisateur est invité à informer la structure habilitée des dysfonctionnements qu'il constate dans le dispositif de filtrage.

A



L'utilisateur est aussi informé que sa boîte de messagerie électronique est la propriété de SONATRACH. Celle-ci se réserve le droit d'accéder à son contenu par le biais d'une demande formelle émanant du responsable n-1 du Président Directeur Général dans le cadre d'un besoin professionnel ou d'une procédure disciplinaire ou juridique.

I.9. UTILISATION D'INTERNET

SONATRACH met à la disposition des utilisateurs un accès à internet dans le cadre de l'exercice de leurs fonctions. L'utilisateur est informé que pour des raisons de sécurité et d'éthique l'accès à certains sites ou services internet peut être limité ou prohibé par la Société.

I.9.1. REGLES DE BON USAGE DE LA NAVIGATION SUR INTERNET

Lors de la navigation sur internet via le réseau de la Société, l'utilisateur doit :

- Se connecter exclusivement à travers la connexion sécurisée que SONATRACH met à sa disposition ;
- Se conformer aux lois en vigueur, en particulier celles relatives aux publications à caractère injurieux, raciste, pornographique et diffamatoire ainsi que celles liées à la :
 - Préservation de l'ordre public, la défense et la sécurité publique ;
 - Préservation de la dignité et la vie privée d'autrui ;
 - Protection des enfants.
- Faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les forums de discussions, recommandés par la Société ou dont l'accès est motivé par des raisons de services. Aussi, s'abstenir d'émettre des opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à la Société ;
- Faire preuve de parcimonie dans l'utilisation des services internet payants mis à disposition par la Société ; *(à titre d'exemple : l'accès aux banques de données pétrolières dont le mode de paiement est fait par nombre d'articles téléchargés).*

L'utilisateur ne doit pas :

- Utiliser internet pour divulguer, publier ou rendre accessible des données classifiées de la Société ;
- Rendre accessible des données de la société, classifiées en particulier, via des sites internet qui offrent des services en ligne tels que la traduction linguistique, la conversion de formats de fichiers, le changement de mot de passe de fichiers ou autres ;
- Donner accès à des tiers, aux abonnements en ligne de revues et bases de données techniques contractés par la Société ;
- Contourner les restrictions d'utilisation d'internet mises en place par SONATRACH, notamment dans le but de :
 - Se livrer à une activité personnelle ou à des fins lucratives ;
 - Accéder à des sites douteux, aux pratiques illégales très souvent vecteur de propagation de Malwares ;
 - Diffuser, télécharger des données, des logiciels ou du contenu multimédia protégés par le droit de propriété intellectuelle ;
 - Prendre part à des jeux en ligne ou à des paris.



I.9.2. UTILISATION A DES FINS PERSONNELLES

L'utilisation de l'internet fourni par SONATRACH à des fins personnelles n'est tolérée qu'à titre exceptionnel et limité dès lors qu'elle ne remette pas en cause ni le bon fonctionnement du service internet ni sa sécurité. Cette utilisation ne doit évidemment pas impacter le rendement de l'utilisateur sous quelque forme que ce soit.

L'utilisation à des fins personnelles reste, cependant, soumise aux mêmes règles de bon usage édictées dans le point I.9.1. SONATRACH se réserve le droit de limiter, à tout moment, ou interdire l'usage d'internet à des fins personnelles.

I.9.3. UTILISATION DES RESEAUX SOCIAUX

Les réseaux sociaux sont des outils de communication et de collaboration, largement utilisés. SONATRACH, à l'instar des entreprises, exploite les multiples avantages des réseaux sociaux à bon escient. L'utilisateur est responsable de l'usage des réseaux sociaux, il est tenu de respecter les règles citées ci-après.

L'utilisateur doit :

- S'abstenir de porter préjudice à la Société par la publication de contenu de nature à nuire à son image ou à celle de ses employés ;
- Se conformer à l'obligation de réserve vis-à-vis de la Société, notamment lorsqu'une publication cite une entreprise partenaire ou concurrente ;
- Respecter les Conditions Générales d'Utilisation (CGU) des réseaux sociaux utilisés ;
- Veiller à vérifier la véracité de l'information et sa source pour ne pas faire office de relayer des Hoax.

L'utilisateur ne doit pas :

- Partager des données professionnelles ou tout autre contenu multimédia de la Société, notamment via messageries instantanées grand public ;
- Utiliser son adresse de messagerie professionnelle pour s'identifier ou s'inscrire sur des réseaux sociaux à titre personnel ;
- Fournir des informations liées à sa position au sein de la Société telles que sa fonction, son grade ou responsabilité sur les réseaux sociaux non professionnels notamment, lors du renseignement des formulaires d'inscription ;
- Propager des Malwares. Le fait de faire suivre ou de cliquer sur des publications douteuses pourrait nuire à la sécurité du poste de travail et du système d'information de la Société. ;

I.9.4. SUPERVISION DE LA NAVIGATION INTERNET

L'utilisateur est informé qu'un dispositif de supervision et de filtrage est mis en place par la Société pour s'assurer du bon fonctionnement du service internet et contrôler son utilisation. Le dispositif permet d'enregistrer tous les accès aux sites effectués par les utilisateurs. L'analyse de ces accès permet à SONATRACH de disposer de statistiques sur les sites visités, les durées des accès des utilisateurs ainsi que les éventuelles tentatives d'accès non autorisées.



I.10. UTILISATION DES EQUIPEMENTS INFORMATIQUES

I.10.1. EQUIPEMENTS INFORMATIQUES MIS A DISPOSITION PAR SONATRACH

Chaque utilisateur est responsable des équipements informatiques mis à sa disposition pour l'exercice de ses fonctions.

L'utilisateur doit :

- Veiller à leur bon fonctionnement et ne pas dégrader leur état ;
- Signaler tout dysfonctionnement à la structure habilitée.

L'utilisateur ne doit pas :

- Intervenir personnellement ou via un tiers, sur l'équipement informatique pour réparation, ou modification de configuration. La maintenance des équipements informatiques est assurée exclusivement par la structure habilitée ;
- Déplacer l'équipement informatique sans accord de la structure habilitée.

I.10.2. REGLES DE SECURITE DES EQUIPEMENTS INFORMATIQUES

L'utilisateur doit :

- Verrouiller l'accès au poste de travail en cas d'absence, même de courte durée ;
- Eteindre les équipements informatiques pendant les absences prolongées (*nuit, weekend, congé, etc.*), sauf besoin spécifique.

I.10.3. REGLES DE SECURITE DES EQUIPEMENTS MOBILES

Les équipements mobiles ne sont octroyés que pour des besoins de service. Les utilisateurs dotés d'équipements mobiles doivent respecter les règles suivantes citées ci-dessous.

L'utilisateur doit :

- Veiller à verrouiller les équipements mobiles lorsqu'ils ne sont pas utilisés ;
- Modifier le code PIN de base des smartphones et tablettes à la première utilisation ;
- Désactiver la fonction d'association automatique aux points d'accès Wifi afin de garder le contrôle sur l'activation de la connexion Wifi ;
- Eviter de se connecter à des réseaux Wifi publics et non sécurisés ;
- Utiliser avec précaution la lecture des Codes QR pour éviter d'être victime d'actes malveillants.

L'utilisateur ne doit pas :

- Laisser l'équipement mobile sans surveillance, s'assurer qu'il n'est pas laissé en évidence, et si possible, le conserver dans un endroit sécurisé lorsqu'il n'est pas utilisé ;
- Stocker les données classifiées sur les équipements mobiles et les supports amovibles, sauf pour nécessité de transport, elles doivent être immédiatement supprimées après ;
- Stocker son mot de passe en clair sur l'équipement mobile (*exemple : dans un fichier lisible*) ;
- Connecter l'équipement mobile ou support amovible en dehors de la Société à un quelconque périphérique ou réseau qui ne soit pas de confiance ;



- Procéder au débridage de l'équipement mobile notamment, par le biais des logiciels de rooting ou jailbreak ;
- Installer des logiciels ou des applications sans un préalable accord de la structure habilitée, notamment les applications provenant d'App Store tel que Google Play, fichiers APK, IPA, ect. ;
- Prêter l'équipement mobile ou le support amovible sans l'accord de la structure habilitée ;
- Désactiver la fonction de verrouillage de l'écran (*exemple : le code PIN, le schéma de déverrouillage de l'écran*) afin d'empêcher tout accès non autorisé ;
- Connecter tout support amovible dont l'origine n'est pas connue ou pas sûre ;
- Brancher l'équipement mobile à un chargeur inconnu ;
- Activer le Bluetooth sauf en cas de besoin ;
- Laisser l'équipement mobile visible lors de l'activation du Bluetooth et rejeter toute sollicitation inattendue.

I.10.4. RESTITUTION DES EQUIPEMENTS INFORMATIQUES

L'utilisateur doit :

- Restituer l'équipement informatique en cas de : mutation, fin de fonction, départ (démission, licenciement, retraite, fin de contrat de travail), détachement ou mise en disponibilité, ainsi que dans le cadre de réparation ou remplacement ou fin d'une mission de travail, fin de stage ou fin de prestation ;
- Déplacer toutes les données à caractère professionnel présentes sur l'équipement informatique, vers l'espace de stockage sécurisé fourni par la structure habilitée ;
- Supprimer les données privées stockées sur l'équipement informatique. La structure habilitée n'est pas responsable de la conservation ou de la confidentialité de ses données privées.

I.10.5. DECLARATION DE PERTE OU DE VOL D'EQUIPEMENTS MOBILES

L'utilisateur doit signaler, à la structure habilitée toute perte ou vol d'équipement mobile ou support amovible professionnel. Dans le cas où la perte ou le vol se produit à l'extérieur de la Société, l'utilisateur est tenu de joindre une copie de la déclaration de perte ou de vol déposée auprès des autorités compétentes ;

L'utilisateur est informé que l'équipement mobile peut faire l'objet de géolocalisation, de verrouillage, de réinitialisation ou de suppression de données à distance.

I.10.6. UTILISATION D'EQUIPEMENTS INFORMATIQUES A DES FINS PERSONNELLES

L'usage des équipements informatiques fournis par la Société à des fins personnelles est toléré dans la stricte mesure où il demeure exceptionnel et doit obéir aux conditions suivantes.

L'utilisateur ne doit pas :

- Entraver ou interférer avec l'activité professionnelle ;
- Configurer de messagerie électronique et instantanée personnelles sur les smartphones et tablettes ;
- Exercer une activité commerciale privée, de divertissement ou politique ;



- Générer des coûts supplémentaires pour la Société par l'usage abusif de consommables.

I.10.7. EQUIPEMENTS INFORMATIQUES PERSONNELS

À l'exception du réseau Wifi visiteur, la connexion d'un équipement informatique personnel au système d'information de SONATRACH est interdite et requiert l'autorisation de la structure habilitée.

L'utilisateur doit :

- Configurer les paramètres de synchronisation pour une durée limitée de conservation des messages, afin de limiter le stockage des données de la Société sur l'équipement informatique personnel ;
- Supprimer de son équipement personnel, les pièces jointes reçues dans la messagerie professionnelle et téléchargées sur celui-ci, après leurs consultations ;
- Supprimer les données professionnelles de l'équipement informatique personnel en cas de cessation de la relation de travail ;
- Supprimer les données professionnelles de l'équipement informatique personnel en cas de cession ou de vente de l'équipement informatique personnel.

L'utilisateur ne doit pas :

- Stocker les données classifiées sur des équipements informatiques personnels ;
- Configurer la messagerie professionnelle sur l'équipement informatique personnel, sauf si les mesures suivantes sont appliquées :
 - Protection par un code PIN, mot de passe ou schéma ;
 - Mise à jour en terme de correctifs de sécurité ;
 - Installation d'un antivirus à jour.
- Prêter l'équipement informatique personnel à des tiers pouvant avoir accès à la messagerie ou aux données professionnelles ;
- Synchroniser la messagerie professionnelle avec le Cloud public.

I.10.8. CONTROLE & SUPERVISION DES EQUIPEMENTS INFORMATIQUES

L'utilisateur est informé qu'il peut faire l'objet de supervision des accès au système d'information de la Société. Cette dernière peut utiliser toutes les méthodes de supervision et de contrôle à sa disposition pour veiller à la sécurité de son système d'information.

I.11. PROTECTION CONTRE LES MALWARES

L'introduction délibérée d'un Malware dans le système d'information de SONATRACH constitue une infraction. Les Malwares peuvent s'introduire dans un système d'information par différents moyens, notamment par support amovible (*clé USB, et autres*), logiciel non autorisé, messagerie électronique, internet, etc.

L'utilisateur est tenu de respecter et de se conformer aux règles de sécurité mises en place par la structure habilitée afin de préserver les données et les ressources du système d'information et de lutter contre les Malwares et les cyberattaques.

L'utilisateur doit :

- Signaler tout comportement anormal ou suspect ou toute anomalie détectée au niveau de son équipement informatique notamment :

A



- Blocage ;
- Ouverture intempestive de fenêtres à l'écran ;
- Affichage et disparition immédiate de boîtes de dialogue au démarrage ;
- Message d'erreur cyclique et récurrent ;
- Présence de fichiers inconnus (film, musique, etc.) ;
- Lenteur inexplicée.
- Etre attentif aux messages d'alerte de son antivirus ;
- Contribuer à atténuer la propagation de Malwares en n'activant pas les macros sur les produits offices ou autres, qu'en cas de besoin ;
- Se prémunir contre d'éventuelles pertes de fichiers importants qui peuvent être occasionnées par ransomwares, en les stockant sur les espaces de stockage sécurisés fournis par la structure habilitée ;
- Veiller à soumettre à la structure habilitée, pour analyse virale, toute clé USB ou autre support amovible fourni par des tiers ou exploité en dehors du système d'information de SONATRACH, avant son utilisation ;
- Etre très attentif aux alertes et notes de sensibilisation communiquées par la Société sur la sécurité des systèmes d'information.

L'utilisateur ne doit pas :

- Installer de logiciels, sans autorisation de la structure habilitée, qui peuvent être un vecteur de propagation de Malwares ;
- Installer des plugins supplémentaires, sur le navigateur internet sans autorisation de la structure habilitée, qui peuvent véhiculer des malwares ;
- Modifier la configuration de son navigateur internet fourni par la Société ;
- Tenter de désactiver, désinstaller ou supprimer l'antivirus fourni par la Société ;
- Cliquer sur les publicités qui s'affichent sur les pages web ;
- Opérer des téléchargements illicites (logiciels craqués, œuvres protégées...) très souvent vecteurs de propagation de Malwares.

I.12. DONNEES PRIVEES

L'utilisateur est informé que SONATRACH se réserve le droit d'accéder à toutes les données stockées dans son système d'information ou sur tout autre support amovible connecté au système d'information de la Société. À ce titre, SONATRACH recommande aux utilisateurs d'user de leurs équipements informatiques personnels pour stocker des données privées et ce, pour le respect de leur vie privée.

Néanmoins, l'utilisation du système d'information de la Société pour créer et stocker des données privées est tolérée, dans la limite d'une utilisation raisonnable, à condition de ne pas :

- Nuire au bon fonctionnement du système d'information ;
- Porter préjudice aux intérêts et à l'image de marque de la Société ;
- Entraver l'exercice des fonctions de l'utilisateur ;



- Engendrer des coûts supplémentaires pour la Société.

Pour revêtir le caractère privé, les données doivent être répertoriées dans un dossier particulier créé à cet effet par l'utilisateur sur son poste de travail et nommé explicitement « **Privé** ».

Exceptionnellement, en cas de risque ou d'événement particulier (*circonstance exceptionnelle*), notamment dans le cas de fuite de données classifiées, d'atteinte à la sécurité de la Société, d'activité illicite ou d'enquête judiciaire, SONATRACH peut être amenée à consulter des données répertoriées dans des dossiers nommés « Privé » avec ou sans la présence ou l'accord préalable de l'utilisateur concerné.

L'accès à ces données, se fera conformément aux dispositions des lois en vigueur.

I.13. ACCES A DISTANCE VIA VPN

La connexion à distance, via VPN, permet à l'utilisateur d'avoir accès aux ressources du système d'information de la Société.

L'utilisateur est informé que l'accès à distance via VPN, au système d'information de SONATRACH n'est pas systématique. L'accès est accordé pour des raisons de service, notamment dans le cas d'un télétravail. L'ensemble des règles de la présente charte sont applicables aux utilisateurs accédant via VPN, au même titre que ceux qui accèdent à partir de leur lieu de travail.

L'utilisateur qui accède, via VPN, au système d'information de SONATRACH doit :

- Utiliser exclusivement les équipements informatiques fournis par la Société ;
- S'engager à en faire un usage strictement professionnel et à ne pas partager son accès avec des tiers.

I.14. MESURES DE SECURITE LORS DES DEPLACEMENTS HORS SOCIETE

Les équipements mobiles et les supports amovibles utilisés lors des déplacements hors Société, sont exposés au risque de vol ou de perte. L'utilisateur est tenu d'être très vigilant et de respecter les règles de sécurité citées ci-après.

L'utilisateur doit :

- Veiller à ne se déplacer qu'avec les données nécessaires à la mission ;
- Éviter de se déplacer avec des données classifiées et privilégier plutôt leur récupération à distance de manière sécurisée ;
- Veiller à vérifier que les logiciels, de sécurité en particulier, sont à jour ;
- Veiller à marquer les équipements mobiles par des signes distinctifs (*exemple : pastille de couleur*) pour une surveillance aisée. Penser à mettre également un signe sur les housses ;
- S'assurer de l'authenticité du réseau wifi public (*Aéroport, hôtel, ...*) en confirmant les paramètres de connexion exacts avec le personnel concerné, la connexion via réseau mobile est à privilégier lors des déplacements au niveau national ;
- Eviter de manipuler des données classifiées lors de l'utilisation d'une connexion wifi publique ;



- Faire très attention aux échanges de documents (*via clé USB lors de présentations commerciales ou de séminaires*). Privilégier des clés dédiées à ces échanges ;
- Veiller à une consommation rationnelle des données mobiles lors des déplacements à l'étranger ;
- Informer la structure habilitée et la représentation diplomatique Algérienne en cas de vol, d'inspection ou de saisie des équipements mobiles ou supports amovibles de la Société par des autorités étrangères lors des déplacements professionnels à l'étranger.

L'utilisateur ne doit pas :

- Laisser les équipements mobiles et les supports amovibles dans des lieux publics, sans surveillance ;
- Utiliser des équipements autres que ceux fournis par SONATRACH pour accéder au système d'information de la Société.

À la fin de la mission et avant le retour, l'utilisateur doit :

- Transférer les données professionnelles vers le système d'information de la Société via connexion sécurisée VPN ou autre ;

Au retour au lieu du travail, l'utilisateur doit :

- Changer les mots de passe utilisés lors de son déplacement ;
- Veiller à scanner au préalable les équipements mobiles et support amovibles avant de les connecter au réseau de la Société.

I.15. DROITS DE PROPRIETE INTELLECTUELLE

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

L'utilisateur s'oblige en toutes circonstances à se conformer à la législation en vigueur qui protège, notamment les droits de propriété intellectuelle. Le manquement au respect de ces droits par l'utilisateur engage sa responsabilité civile et même pénale aux yeux du droit Algérien.

SONATRACH veille au respect des droits de propriété intellectuelle, elle ne peut être tenue responsable de délits commis par un utilisateur dans ce domaine.

Toute création ou œuvre intellectuelle produite par l'utilisateur dans le cadre professionnel est considérée comme propriété intellectuelle de SONATRACH.

I.16. MANQUEMENT AU RESPECT DE LA CHARTE ET SANCTIONS

Le manquement de l'utilisateur au respect des règles édictées dans la présente charte engage sa responsabilité et peut entraîner à son encontre des limitations ou suspensions d'utiliser tout ou une partie des ressources du système d'information, un avertissement verbal voire des sanctions disciplinaires proportionnées à la gravité des faits constatés. Ces mesures peuvent aller d'un blâme au licenciement conformément aux dispositions du règlement intérieur de SONATRACH.



N° 536 /DG

Classement : 0.007.5/20

Référence : E-023 (R1)

Page : 16 de 16

SONATRACH, par le biais de son représentant légal, se réserve le droit d'engager des poursuites judiciaires indépendamment des sanctions disciplinaires mises en œuvre dans son Règlement Intérieur, notamment en cas d'infraction, de non-respect de propriété intellectuelle ou de violation du secret professionnel.

Fait à Alger, le 11 NOV. 2020

Le Président Directeur Général,

T. HAKKAR

