

CHARTE INFORMATIQUE DE L'INERIS

SOMMAIRE

1	POURQUOI CETTE CHARTE ?	4
1.1	introduction	4
1.2	Champ d'application	4
1.3	Modalités de diffusion de la charte	4
1.4	Usages concernés	4
1.5	Terminologie	5
1.6	Suivi des évolutions	5
2	LES INTERLOCUTEURS.....	6
2.1	La direction des ressources humaines	6
2.2	La direction des systèmes d'information	6
2.3	Le support informatique	6
2.4	La hiérarchie.....	6
3	LES PRINCIPES GENERAUX : L'UTILISATEUR EST RESPONSABLE DE CE QUI LUI EST CONFIE	7
4	LE POSTE DE TRAVAIL	8
4.1	Attribution du poste de travail.....	9
4.2	Travaillez confortablement	9
4.3	Organisez vos documents	9
4.4	N'utilisez que les périphériques fournis par la DSI de l'INERIS.....	9
4.5	Cas particulier du micro-ordinateur portable.....	10
4.6	Protection des données STOCKEES à caractère personnel	10
4.7	En cas de vol ou perte de matériel	11
4.8	Cas particulier du prêt de matériel	11
4.9	Usage du poste de travail à des fins personnelles	11
5	LES MOYENS D'IMPRESSION	12
5.1	Des moyens d'impression multifonctions réseaux sont à la disposition des utilisateurs.	12
5.2	Les principes fondamentaux à respecter	12
6	LA MESSAGERIE ELECTRONIQUE	12
6.1	Responsabilité	13
6.2	Outil professionnel, usage personnel	13
6.3	Déontologie.....	14
6.4	Signature des messages	14
6.5	MAITRISE DE LA COMMUNICATION PAR LA MESSAGERIE	14

6.6	Envoi en nombre	14
6.7	Les pièces jointes	15
6.8	Messages et documents à détruire.....	15
6.9	Archivez vos messages.....	15
6.10	Gestion des spams.....	15
7	INTERNET	16
7.1	Moyens d'accès	16
7.2	Usages.....	16
7.3	Accès Web	16
7.4	E-Réputation et utilisation des réseaux sociaux	16
7.5	Filtrage et règles de traçabilité.....	17
8	LA SECURITE.....	18
8.1	Le mot de passe	18
8.2	Responsabilité	19
9	LA TELEPHONIE	20
9.1	Téléphone portable personnel	20
9.2	Téléphone portable professionnel.....	20
10	DEVELOPPEMENT DURABLE	21
11	L'USAGE DES TERMINAUX PRIVES A DES FINS PROFESSIONNELLES	21
12	ABSENCE PROLONGEE / DEPART DE L'INERIS	22
12.1	Absence prolongée.....	22
12.2	Départ de l'INERIS	22
12.3	Cas particulier d'un départ soudain d'un employé	22
13	VIE PRIVEE / DROIT A LA DECONNEXION	23
14	RESPONSABILITES - SANCTIONS.....	23
14.1	Contrôle et audit	24

1 POURQUOI CETTE CHARTE ?

1.1 INTRODUCTION

L'INERIS met à disposition de ses employés un ensemble de moyens informatiques et de communication nécessaires à l'exercice de leurs missions.

Cette charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de l'institut. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite.

Le respect par chaque collaborateur de cette charte contribue ainsi à le protéger ainsi que l'INERIS face aux risques et conséquences qui peuvent être induits par la méconnaissance, l'imprudence, la négligence ou la malveillance et qui sont de nature :

- D'une part, à nuire gravement au bon fonctionnement et/ou à l'image de l'INERIS
- D'autre part, à engager sa responsabilité civile et/ou pénale ainsi que celle de l'INERIS.

La charte s'appuie sur la législation nationale et européenne et est également conforme aux différentes recommandations de la Commission Nationale Informatique et Libertés.

La charte rassemble les consignes qui doivent être appliquées ainsi que les conseils et recommandations de bon usage. Les manquements à ces consignes peuvent être sanctionnés sur le terrain de la responsabilité disciplinaire, sans préjudice de possibles recours sur le plan civil ou pénal.

Dès lors que la charte est publiée, accessible à tous les utilisateurs, et entrée en vigueur, elle constitue un document applicable et opposable aux salariés sans nécessité de consentement.

L'utilisateur est alors réputé en avoir pris connaissance et l'appliquer.

1.2 CHAMP D'APPLICATION

La charte concerne tous les employés de l'EPIC INERIS ainsi que les personnes (partenaires, prestataires, stagiaires, etc..) habilitées par la DSI qui utilisent des ressources informatiques et de communication fournis par l'INERIS EPIC. Le terme « utilisateur » est employé de manière générique, pour les représenter dans l'ensemble de la charte.

La présente charte s'applique donc à tout utilisateur ayant le besoin d'accéder aux systèmes d'information de l'INERIS dans le cadre de l'exercice de ses missions.

1.3 MODALITES DE DIFFUSION DE LA CHARTE

La Politique de sécurité des systèmes d'information (PSSI) de l'INERIS mentionne que chaque utilisateur s'engage à connaître et à appliquer l'ensemble des dispositions de la présente charte.

Elle est systématiquement remise à tout nouvel arrivant et est annexée au règlement intérieur de l'INERIS.

Elle fait l'objet d'une clause spécifique dans les contrats liant l'institut à des partenaires.

Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques exigées ou recommandées.

1.4 USAGES CONCERNES

La présente charte s'applique à tous les types d'usage qu'ils aient lieu :

- dans les locaux de l'INERIS;
- dans les locaux tiers dans lesquels l'INERIS exerce ses missions ;

- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès.

La présente charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des moyens informatiques et de communication électronique.

1.5 TERMINOLOGIE

Abréviations - Termes	Définitions
Utilisateur	Toute personne utilisatrice d'un poste de travail ou de tout autre moyen informatique ou de communication de l'INERIS
Système d'information	Véhicule de la communication dans l'organisation. Sa structure est constituée de l'ensemble des ressources (les hommes, le matériel, les logiciels) organisées pour : collecter, stocker, traiter et communiquer les informations.
Poste de travail	Ordinateurs et moyens de téléphonie, impression, édition, télécopie, mis à disposition des utilisateurs pour accomplir leurs missions.

1.6 SUIVI DES EVOLUTIONS

La présente charte fait l'objet de mises à jour présentées aux représentants des personnels en fonction des évolutions suscitées par les éléments suivants :

- Changement dans le niveau de classification des informations traitées ;
- Modification du mode d'exploitation ;
- Modification des objectifs de sécurité (menaces, vulnérabilités ...) ;
- Modification ou remplacement des moyens de protection, des équipements ;
- Modification importante de l'environnement du système (ex : changement de mode d'hébergement) ;
- Evolutions fonctionnelles importantes du système ;
- Résultats non satisfaisants d'une inspection ou d'un audit de sécurité ;
- Occurrence d'un incident de sécurité majeur, rapport d'analyse d'incident ;
- Modification du mandat de l'INERIS dans la réalisation de ses missions par son ministère de tutelle ;
- Evolution de la réglementation en vigueur (ministère de tutelle, etc.).

La dernière version actualisée et en vigueur, la seule faisant foi, est enregistrée dans le système de gestion de la documentation qualité. Elle est consultable par l'ensemble du personnel.

Le personnel de l'INERIS en est averti par courrier électronique et par sa hiérarchie.

2 LES INTERLOCUTEURS

2.1 LA DIRECTION DES RESSOURCES HUMAINES

La direction des ressources humaines est garante de la fourniture à tout employé des moyens nécessaires à l'accomplissement de son travail.

A ce titre, elle s'assure auprès de la DSI de la cohérence des moyens informatiques fournis aux utilisateurs et de leur utilisation dans un cadre légal de travail.

Le directeur des ressources humaines répond à la direction générale de la bonne application de la présente charte par les employés.

2.2 LA DIRECTION DES SYSTEMES D'INFORMATION

Sous le terme générique de « services informatiques », les différents services en charge des systèmes d'information de l'institut ont pour vocation de mettre à disposition des utilisateurs un ensemble de moyens techniques leur permettant d'utiliser dans les meilleures conditions les technologies du traitement de l'information.

Ils doivent en outre veiller à ce que ce système d'information soit cohérent, pérenne, sécurisé, disponible et évolutif.

Les moyens techniques sont affectés par la DSI selon les besoins de l'utilisateur dans l'exercice de sa mission et sont ajustés en fonction de l'évolution de cette dernière.

Le responsable hiérarchique de chaque entité répond à la direction générale des éléments techniques concourant à la mise en application de la présente charte.

Les services informatiques sont également maîtres d'œuvre des évolutions de la charte.

2.3 LE SUPPORT INFORMATIQUE

Le support informatique a en charge le support à l'utilisateur, les dépannages, qu'il s'agisse de problèmes de matériel ou de logiciel. Il peut également apporter conseil, assistance et accompagnement. Le point d'entrée du support informatique est matérialisé par l'équipe « SUPPINFO ».

Ainsi, si l'utilisateur rencontre des difficultés sur les systèmes d'information de l'institut, il doit contacter impérativement cette équipe dédiée à l'assistance au [6666].

Ce point de contact unique garantit que la demande est répertoriée, tracée et que les actions de correction et/ou d'évolution seront conduites. Par ailleurs, cela permet de répercuter le cas échéant les actions correctives ou évolutions aux autres utilisateurs.

L'utilisateur peut également saisir sa demande en envoyant un courriel au service «SUPPINFO ».

Pour apporter un meilleur service, le support informatique, le cas échéant relayé par un autre administrateur des services informatiques, peut utiliser un logiciel de prise en main à distance pour pouvoir intervenir plus rapidement sans avoir à se déplacer sur le poste. L'utilisation de cet outil requiert l'autorisation de l'utilisateur concerné au moment du traitement du problème rencontré.

Avant la prise en main, l'utilisateur doit valider (sur son écran) qu'il autorise l'accès à son poste de travail. Celui-ci ne peut donc se faire qu'après acceptation de l'utilisateur. Tout au long de l'opération de prise en main une icône apparaît sur l'écran de l'utilisateur.

2.4 LA HIERARCHIE

La hiérarchie de l'utilisateur doit être son interlocuteur privilégié pour toute problématique liée à ses besoins d'équipements et moyens. Il appartient à la hiérarchie de s'assurer de l'adéquation entre les exigences des missions de l'utilisateur et des moyens sollicités, en lien avec les éléments de la fiche de poste.

3 LES PRINCIPES GENERAUX : L'UTILISATEUR EST RESPONSABLE DE CE QUI LUI EST CONFIE

Le poste de travail est la propriété de l'INERIS et appartient à son patrimoine. Il est mis à disposition de l'utilisateur afin de lui permettre d'assurer ses tâches professionnelles et doit être considéré comme un outil de travail et de production.

Les utilisateurs doivent appliquer les principes majeurs suivants :

Principe n ° 1 : Vous devez utiliser votre poste de travail avec les outils et les paramètres validés par la DSI

Ne modifiez pas les outils et les paramètres vous-même au risque de provoquer des dysfonctionnements techniques graves, pouvant conduire à la perte ou au vol de données.

Votre poste a été configuré en fonction de vos missions. Les modifications rendues nécessaires par l'évolution de ce besoin sont opérées uniquement par des employés spécialisés, selon les procédures en vigueur.

Les logiciels installés sur votre poste font l'objet de droits d'usage qui sont régulièrement acquittés. Vous ne devez pas les enlever ou en ajouter, au risque de vous rendre coupable d'un délit de contrefaçon. Exprimez vos besoins éventuels en contactant le support informatique.

De même, l'installation d'un logiciel sur un système informatique mis en œuvre par l'INERIS, dont le droit d'usage est acquis à titre privé par un employé, n'est pas autorisée.

L'usage de logiciels commerciaux est régi par des contrats et protégé par des lois qui entraînent une responsabilité personnelle de leurs utilisateurs, que la responsabilité propre de l'institut en tant que personne morale ne saurait exonérer.

Toute utilisation ou installation complémentaire doit faire l'objet d'une validation par la DSI, et éventuellement des directions opérationnelles (notamment concernant les logiciels scientifiques).

Ainsi, vous ne devez pas utiliser de logiciel complémentaire y compris « portables » sans validation préalable de la DSI, même si ce logiciel ne nécessite pas de privilèges pour s'exécuter ou s'installer.

La configuration de votre poste est inventoriée et tenue à jour dans une base de données de gestion de parc : description du matériel, des logiciels installés, des accès à des applications distantes, etc...

Principe n° 2 : Vous êtes responsable de l'information qui vous est confiée

Les données informatiques et les informations qu'elles contiennent, constituent le patrimoine immatériel de l'institut. A ce titre, vous devez prendre des précautions pour veiller à leur sécurité, c'est-à-dire leur disponibilité, leur intégrité mais aussi leur confidentialité.

Chaque employé est responsable des informations qu'il divulgue à l'extérieur.

A ce titre, il est attendu qu'il veille à ne pas communiquer d'informations sensibles voire confidentielles sans s'être au préalable assuré qu'il est dûment habilité pour le faire.

Parmi ces informations sensibles on peut compter des informations pouvant mettre en péril la sécurité, l'intégrité, la compétitivité, la réputation ou la stratégie de l'INERIS.

Principe n° 3 : Vous utilisez l'ensemble des moyens informatiques de la façon prévue, pour l'usage prévu

En particulier, vous ne devez pas installer ou utiliser de logiciels sans lien direct avec le contexte professionnel (jeux, etc.), ou effectuer des travaux qui n'entrent pas dans votre cadre de travail.

Seuls, le téléchargement et le stockage de musiques, photos, films... ayant trait à l'activité professionnelle sont autorisés. En cas de besoin s'adresser au support informatique.

Principe n° 4 : Vous pouvez utiliser votre poste de travail à des fins privées, mais de manière exceptionnelle

L'utilisation du poste de travail à titre privé est tolérée à des fins exceptionnelles et à condition qu'elle ne constitue pas une infraction aux présentes instructions et aux dispositions légales, et ne nuise en rien à la sécurité des systèmes d'information. De même, un usage exceptionnel du système de messagerie de l'INERIS à des fins privées est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels et qu'il ne constitue pas une infraction aux présentes instructions et aux dispositions légales. Les messages privés doivent comporter dans leur objet la mention « personnel » ou « perso ». Dans tous les cas, cette utilisation ne doit pas nuire à la sécurité et à la fluidité du trafic.

De plus, l'accès à certains sites non professionnels peut conduire à des téléchargements, volontaires ou non, de programmes pouvant contenir des virus, des programmes potentiellement dangereux, destructeurs ou divulgateurs d'informations, notamment celles qui concernent directement l'INERIS.

Dans le cadre de son devoir de loyauté, chaque utilisateur doit veiller à ce que tout échange avec l'extérieur (messagerie, chat, forum, réseaux sociaux, etc. ...) ne porte pas préjudice à l'institut par exemple par la diffusion d'informations n'intéressant pas le public, ou potentiellement confidentielles, la diffusion d'informations erronées ou diffamantes, etc...

Les accès aux sites de divertissement multimédia sont interdits, notamment car ils encombrant la bande passante et ralentissent donc le fonctionnement du réseau. Ils pénalisent ainsi l'ensemble des employés de l'institut. Il en va de même pour les logiciels permettant de télécharger divers médias, qui sont formellement interdits à l'installation sur les postes et à l'usage sur les réseaux de l'INERIS.

Il est interdit de contourner les mesures de sécurité et de filtrage mises en œuvre par l'INERIS.

4 LE POSTE DE TRAVAIL

Le poste de travail est constitué par l'ensemble des moyens affectés à un utilisateur pour réaliser les missions qui lui sont confiées.

Le poste de travail comprend par exemple :

- L'ordinateur : unité centrale, écran, clavier, souris ;
- L'espace réseau et stockage de données ;
- Les logiciels configurés ;
- Les moyens d'impression, édition, numérisation et télécopie, partagés ;
- Le cas échéant : casque, ordinateur portable, ordiphone (tablette, smartphone, ...), moyens d'impression dédiés ;
- etc.

4.1 ATTRIBUTION DU POSTE DE TRAVAIL

La demande initiale d'attribution de matériel et/ou de logiciel par un employé doit être réalisée via le formulaire prévu à cet effet, disponible sur l'intranet et dans le système de gestion de la documentation qualité de l'institut. La demande est transmise à la hiérarchie qui valide le besoin.

Les services informatiques procèdent alors à la mise à disposition des outils informatiques et de communication, sous réserve du respect des règles et contraintes en vigueur (budgets, cohérence technique). Toute demande en dehors de ce circuit sera considérée comme irrecevable.

Les demandes de changement ultérieures sont transmises au service support après validation de la hiérarchie.

Lorsque le besoin ou la mission de l'utilisateur évoluent, la DSI procède aux ajustements justifiés.

4.2 TRAVAILLEZ CONFORTABLEMENT

Soignez l'ergonomie de votre poste de travail pour ne pas engendrer de troubles de la santé tels que fatigue visuelle, troubles musculosquelettiques (pour plus d'information consulter le site de l'INRS).

Par ailleurs, manger et boire à proximité de tout équipement informatique est fortement déconseillé.

4.3 ORGANISEZ VOS DOCUMENTS

Les documents professionnels doivent être gérés et stockés conformément aux éventuels consignes et usages de l'INERIS relatifs à l'activité concernée.

Adoptez des conventions pour les noms de vos fichiers en évitant les caractères accentués, les caractères de ponctuation (?./*% ...).

Veillez à ne pas stocker vos fichiers uniquement sur les disques durs locaux de vos ordinateurs ou autre stockage amovible (disque externe, clef USB...). En effet, sauf exception, les informations stockées sur les PC en local (disque dur) ne sont pas garanties par l'INERIS et ne sont donc pas couvertes par une politique de sauvegarde dédiée. Chaque utilisateur doit donc veiller à leur sauvegarde sur le réseau. Les services informatiques déclinent toute responsabilité en cas de perte de fichier stocké en local.

4.4 N'UTILISEZ QUE LES PERIPHERIQUES FOURNIS PAR LA DSI DE L'INERIS

Une attention particulière doit être portée aux périphériques de stockage externes, qui constituent un vecteur de menaces SSI. En règle générale vous ne devez connecter à votre poste de travail que les périphériques externes préalablement autorisés par la DSI et vous ne devez pas confier ces périphériques à des tiers. L'utilisation des clefs USB ou autres supports amovibles préalablement utilisés ou fournis par des tiers doit faire l'objet d'un examen approfondi avant usage. Ainsi, si possible, ces moyens ne doivent pas être connectés à votre poste de travail avant contrôle préalable par la DSI.

Formulez votre besoin et demandez une dérogation au cas par cas auprès de la DSI si besoin est.

Exceptionnellement, lorsqu'aucun autre moyen n'est à votre disposition et ne pouvait être envisagé au préalable, l'usage d'un stockage amovible externe pour recevoir des fichiers reste possible mais il doit faire l'objet de la plus grande prudence et l'utilisateur doit :

- Exécuter un contrôle anti-virus approfondi et complet du média dès son branchement. Si celui-ci révèle des anomalies, le support de stockage doit être retiré immédiatement et son usage exclu jusqu'à examen par DSI ;
- N'exécuter aucun programme depuis le support USB (sauf logiciels fournis par la DSI) ;

- Faire procéder dès son retour sur site à un examen du support amovible, voire du PC, par le support informatique.

L'utilisateur doit dans tous les cas se conformer aux règles de sécurité en vigueur et consulter dans les plus brefs délais la DSI en cas de doute.

L'envoi de fichiers vers l'extérieur doit être réalisé au travers des seuls moyens mis à disposition par l'INERIS. Les moyens à privilégier sont la messagerie INERIS ou la plateforme sécurisée INERIS pour les fichiers volumineux et/ou confidentiels. Si toutefois vous êtes contraint d'utiliser un stockage amovible (fourni par l'INERIS) pour transmettre des données à des tiers, vous ne devez pas reconnecter ce périphérique à votre PC sans l'avoir au préalable confié à la DSI.

4.5 CAS PARTICULIER DU MICRO-ORDINATEUR PORTABLE

En raison des forts risques de perte de données liés à l'utilisation de moyens mobiles, les disques durs des ordinateurs portables sont cryptés et sauvegardés. Les modalités de sauvegardes sont définies par la DSI.

La souplesse d'emploi de ce type de matériel implique une rigueur d'utilisation concernant :

- Sa manipulation (sensibilité aux chocs) ;
- Son vol ; l'ordinateur doit être physiquement attaché à l'aide du câble antivol prévu à cet effet, en cas d'absence.

L'usage dit « nomade » impose à l'utilisateur en déplacement un niveau de surveillance et de confidentialité renforcé comme suit :

- L'utilisateur doit adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information de l'INERIS qu'il pourrait être amené à manipuler ou à échanger ; notamment, la DSI peut fournir sur demande un filtre de confidentialité ;
- Il doit également veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser, accéder ou corrompre leurs contenus ;
- Avant un déplacement à l'étranger, l'utilisateur doit s'assurer auprès de la DSI des précautions particulières à appliquer sur son matériel informatique (ordinateur dédié, cryptographie, etc...). Ces précautions varient selon la destination et le cadre du déplacement. Pour plus d'information l'utilisateur pourra également consulter le site de l'ANSSI ;
- En cas d'incident avéré ou de doute, l'utilisateur doit immédiatement en aviser la DSI de l'INERIS.

4.6 PROTECTION DES DONNEES STOCKEES A CARACTERE PERSONNEL

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès, de rectification et d'opposition les concernant.

Les employés de l'INERIS souhaitant stocker des données personnelles sur leur poste de travail y sont autorisés, à la seule condition de se conformer aux points suivants :

- Ces données doivent être stockées au sein d'un dossier nommé « Personnel ». Toutes données stockées sur le poste de l'employé en dehors de ce dossier seront considérées comme étant à usage professionnel et donc propriété de l'institut ;
- Le dossier « Personnel » doit être créé sur une partition ou un répertoire bien identifié(e) du disque dur du poste, et en aucune manière sur le bureau, afin d'éviter les problèmes dus à la performance lors des ouvertures de sessions ou aux profils itinérants. Le dossier « Personnel » ne doit en aucune manière être créé sur un espace de partage collaboratif hébergé par les

serveurs de l'INERIS, Les points précédents impliquent les précautions d'usage par l'employé pour la sauvegarde de ses données personnelles. L'Institut n'est en aucun cas garant de la sauvegarde des données à caractère non professionnel ;

- Les données du dossier « Personnel » ne sont accessibles qu'à l'intéressé. Néanmoins, dans le cadre d'une enquête faisant suite à l'observation d'événements pouvant indiquer qu'il existe un risque pour la sécurité des systèmes d'informations de l'INERIS (par exemple en cas de détection d'une activité numérique suspecte) ou de présence de fichiers en contradiction avec la présente charte, l'éthique de l'institut ou la législation, une vérification de son contenu peut être réalisée à la demande du Directeur Général par les personnes habilitées en présence du salarié. Si la présence du salarié est impossible, il sera explicitement informé avant l'intervention ;
- Les informations stockées par les membres des instances représentatives du personnel, ont le même caractère de données personnelles. Elles doivent être sauvegardées dans des lieux de stockage partagé au libellé clair (portant mention « Instances du personnel »).

4.7 EN CAS DE VOL OU PERTE DE MATERIEL

Le vol, la perte de matériel informatique (stations de travail, ordinateurs portables, disques durs, ordiphones et téléphones portables et, plus généralement, tous supports de données) doivent être signalés auprès de la hiérarchie et du support de la DSI par l'utilisateur au plus tard dans les 24 heures après constatation des faits ou dès l'ouverture de l'INERIS si ces faits surviennent en heures non ouvrées.

L'utilisateur devra également fournir la liste la plus précise possible des documents contenus sur les matériels et supports de données disparus.

En complément, tout vol de matériel informatique doit faire l'objet d'un dépôt de plainte à la police ou la gendarmerie par le salarié qui en est dépositaire dans les 24 heures suivant le constat des faits. Le récépissé de plainte est un document administratif obligatoire qui doit être transmis à l'officier de sécurité de l'INERIS.

4.8 CAS PARTICULIER DU PRET DE MATERIEL

L'utilisateur doit renseigner et signer un registre, tenu par le service « SUPPINFO », actant la remise de tout équipement prêté.

Il en assure la garde et la responsabilité ; il doit informer le service « SUPPINFO » en cas d'incident (perte, vol, dégradation, dysfonctionnement) et doit le cas échéant procéder aux démarches telles que la déclaration de vol ou de plainte.

Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces équipements. Le bon retour du matériel et ses accessoires est consigné dans le registre.

4.9 USAGE DU POSTE DE TRAVAIL A DES FINS PERSONNELLES

Les postes de travail sont affectés aux employés dans le but de réaliser leurs missions.

L'usage à des fins privées est toléré et doit respecter des limites. Ces limites sont rappelées dans la présente charte.

5 LES MOYENS D'IMPRESSION

5.1 MOYENS D'IMPRESSION

Afin de rationaliser les moyens d'impression, le système d'information de l'INERIS est équipé de photocopieurs multifonctions, mis à disposition des employés, qui offrent plusieurs services :

- Copieur ;
- Impression ;
- Scanner.

Les moyens installés visent des modes d'impression étendus (recto-verso, plusieurs pages sur une seule, respect de la confidentialité, etc.) et parce qu'ils sont en réseau, offrent aux employés une meilleure disponibilité.

De ce fait, l'usage des imprimantes individuelles est restreint à des cas très spécifiques.

5.2 PRINCIPES FONDAMENTAUX A RESPECTER

Règle n° 1 : mutualiser les moyens inter-directions par la mise en œuvre des impressions en réseau sur les photocopieurs multifonctions (copie, impression, numérisation) et traceurs ;

Règle n° 2 : si le mode sécurisé est disponible, tous les documents confidentiels devront être imprimés par ce biais ;

Règle n° 3 : exploiter les performances technologiques des photocopieurs multifonctions pour traiter les travaux de reprographie ; ne recourir au service de la reprographie que pour des travaux spécifiques qui ne peuvent pas être exécutés par les moyens implantés en local ou qui monopoliseraient l'outil au détriment des autres utilisateurs.

Conformément à la politique d'impression et la politique de développement durable de l'institut, seuls les travaux spécifiques ne pouvant être exécutés sur les moyens d'impression implantés en local (volumes et finitions) devront faire l'objet d'une demande à la reprographie.

6 LA MESSAGERIE ELECTRONIQUE

La boîte aux lettres électronique relève du secret de la correspondance (Art 226-15 du Code pénal).

L'INERIS met à la disposition de chaque utilisateur une adresse de messagerie électronique composée de ses prénom et nom d'usage, ainsi que de l'extension «@ineris.fr». Certaines règles fondamentales doivent être respectées.

Chaque employé possédant une boîte aux lettres (BAL) de la messagerie dispose également d'une adresse e-courriel qui la relie au réseau internet. Il est ainsi en mesure d'échanger des informations (envoi et réception) avec les collègues de l'institut et des adresses extérieures à l'institut. Les personnes qui disposent d'une adresse e-courriel sont répertoriées dans l'annuaire de messagerie électronique.

La consultation de cette adresse professionnelle à partir d'un ordinateur hors réseau de l'INERIS ne doit se faire que via un accès sécurisé autorisé par les services informatiques.

6.1 RESPONSABILITE

Chaque utilisateur est responsable de l'utilisation de sa boîte aux lettres.

Le gestionnaire d'une boîte aux lettres d'un projet ou d'une activité par exemple, ou son suppléant sont responsables de l'usage qu'ils en font. Ils doivent respecter les règles de sécurité du mot de passe.

Le contenu des messages envoyés par les utilisateurs sous leur timbre est de leur responsabilité. Les règles hiérarchiques et d'organisation des pouvoirs internes doivent impérativement être respectées, notamment les signatures et les engagements, tout comme pour un courrier papier.

Un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'INERIS. Cela implique que l'utilisateur doit distinguer clairement dans les messages qu'il envoie les informations officielles de ses options personnelles.

Tout courrier électronique engageant l'institut doit respecter les règles formelles de validation en vigueur à l'INERIS, au même titre que tout autre document émis.

Tout utilisateur a une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations et document électroniques disponibles sur le réseau interne. Ceci implique de s'assurer auprès de sa hiérarchie du niveau de confidentialité des documents avant de les diffuser.

De ce fait, il est interdit de rediriger automatiquement les messages reçus vers une adresse hébergée hors du système de messagerie de l'INERIS.

Le principe de délégation permet à un titulaire de déléguer certaines tâches à son délégataire. La délégation par laquelle le titulaire confie l'usage de sa boîte aux lettres à un ou plusieurs acteurs implique une obligation d'acceptation des délégataires dans la limite de leurs attributions. L'utilisateur qui a délégué la gestion de sa boîte aux lettres à un tiers assume la responsabilité des messages qui sont envoyés via cette boîte.

6.2 OUTIL PROFESSIONNEL, USAGE PERSONNEL

La messagerie est un outil de travail à part entière. L'utilisateur doit la consulter au minimum une fois par jour, hormis en période de congés ou en cas d'impossibilité technique d'y accéder avec les outils fournis par l'INERIS. L'utilisateur doit accorder la même importance aux messages électroniques qu'aux courriers postaux ou fax et se doit de les traiter.

Un usage exceptionnel dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique soit conforme aux dispositions de la présente charte et au droit informatique, qu'elle n'affecte pas le trafic normal des messages professionnels et qu'elle ne gêne en rien les activités du service.

Les employés de l'INERIS doivent se conformer aux points suivants :

- Les messages à caractère personnel doivent en faire explicitement mention dans l'objet, en intégrant la mention « Personnel » ou « Perso ». Ainsi, dans le cadre du droit du respect à la vie privée des employés de l'INERIS, ces messages ne pourront être portés à la connaissance de la hiérarchie, même dans un contexte de contrôle interne (cf. § protection des données personnelles) ;
- La création d'un dossier au sein duquel la correspondance à titre privée entretenue par l'employé est autorisée, celui-ci devra se nommer « Personnel ». Tout message stocké sur la messagerie de l'employé en dehors de ce dossier sera considérée comme étant à usage professionnel et donc propriété de l'institut et notamment, à ce titre, pourra faire l'objet d'un contrôle ;

- Les informations échangées entre/avec les membres des instances représentatives du personnel ont également un caractère de données personnelles. Elles doivent donc être échangées avec un objet portant mention « IRP », « Instances du personnel », « Personnel » ou « Perso ».

L'adresse de messagerie attribuée à un employé ne doit être communiquée à des tiers qu'à des fins professionnelles, et non sur internet par des mailings ou sur des sites web autres que ceux utilisés dans le cadre de sa mission au sein de l'INERIS.

6.3 DEONTOLOGIE

Les règles de courtoisie et de déontologie veulent que l'on ne modifie pas un message reçu avant de le transmettre à un autre destinataire (l'origine du message doit être conservée).

Par ailleurs, il est demandé de limiter l'envoi de courriels en dehors des heures d'ouverture de l'Institut, sauf en cas d'absolue nécessité ou de contraintes spécifiques de service.

6.4 SIGNATURE DES MESSAGES

Tous les messages électroniques envoyés à l'extérieur contiennent la signature de l'expéditeur.

La signature doit respecter le format préconisé par la direction de la communication et notamment comprend :

- Le nom et le prénom de l'expéditeur ;
- Son intitulé de poste ;
- Les mentions, fournies par le service juridique de l'INERIS sur l'usage inapproprié de messages reçus par erreur.

6.5 MAITRISE DE LA COMMUNICATION PAR LA MESSAGERIE

Soyez brefs, clairs et concis. Choisissez vos destinataires avec discernement pour ne transmettre le message qu'aux personnes en ayant réellement besoin. Distinguez absolument les personnes qui doivent vous répondre ou qui doivent agir (destinataires - Dest.) des personnes que vous informez (utilisateurs en copie - CC). Évitez autant que possible d'utiliser les listes électroniques de diffusion. De même, l'objet d'un message se doit d'être pertinent et explicite.

6.6 ENVOI EN NOMBRE

La diffusion massive de messages est susceptible de perturber le bon fonctionnement du réseau. C'est pourquoi il convient de limiter au strict nécessaire les envois en nombre. Les messages doivent être envoyés aux seuls destinataires intéressés et concernés par le sujet. L'envoi d'un message en nombre doit avoir un motif strictement professionnel et ne doit être employé qu'en cas de nécessité.

Les envois en nombre, notamment à destination de l'ensemble du personnel, doivent être effectués en indiquant les destinataires au sein du champ « copie masquée » (Cci), à des fins de confidentialité et de bonne transmission et afin d'éviter les effets de réponse massive.

Les listes de diffusion

Des listes de diffusion existent, regroupant des personnes d'une même entité (direction, service, groupe de travail ...).

L'utilisation de ces listes doit être circonscrite à un usage professionnel et réservée à la diffusion d'informations intéressant l'ensemble des membres de la liste.

Les réponses aux envois en nombre

Les messages envoyés en nombre appellent rarement une réponse. Le cas échéant, l'utilisateur veillera à répondre uniquement à l'auteur du message et non à l'ensemble des destinataires.

Les destinataires qui utilisent, pour répondre à un message illicite, la fonction « répondre à tous » sont aussi fautifs que l'émetteur initial et passible d'un rappel au bon usage de la messagerie.

6.7 PIECES JOINTES

Vous devez restreindre le nombre de pièces jointes au strict nécessaire et exploiter au maximum les capacités d'espaces de stockage commun offertes par l'INERIS. Si vous avez besoin d'échanger des fichiers avec des utilisateurs externes identifiés, il est préférable d'utiliser la plateforme d'échange sécurisée INERIS prévue à cet effet.

D'autre part, vous ne devez pas transmettre de programmes informatiques : ceux-ci font l'objet d'une licence d'utilisation et doivent être installés suivant des règles précises. Transmettre des fichiers exécutables ou fichiers sources par courriel est à éviter, pour des raisons de sécurité, de conformité réglementaire ou de propriété intellectuelle.

6.8 MESSAGES ET DOCUMENTS A DETRUIRE

La loi interdit le stockage et la diffusion de messages ou documents de nature diffamatoire, discriminatoire, pédophile ou incitant à la violence ou à la haine raciale. Par conséquent, si un utilisateur reçoit des messages ou des documents de cette nature, il doit :

- Alerter le directeur des systèmes d'information qui engagera les actions nécessaires ;
- Effacer les documents de sa messagerie ou de son disque dur.

Le stockage de documents de cette nature sur un équipement de l'institut constitue une faute grave passible de sanctions disciplinaires, voire pénales.

6.9 ARCHIVEZ VOS MESSAGES

Pour des raisons d'encombrement des systèmes informatiques, la taille de votre boîte aux lettres est limitée. Pour éviter d'être bloqué et économiser de l'énergie, supprimez les messages inutiles ou obsolètes et archivez ceux que vous jugez utile de conserver (si nécessaire, contactez le support pour connaître la procédure à suivre).

Au cas par cas, dûment justifié, la taille limite de la boîte aux lettres peut être augmentée par la DSI.

6.10 GESTION DES SPAMS

L'INERIS utilise un dispositif visant à éliminer les messages indésirables (spams). Lorsque des spams vous sont adressés, ceux-ci sont placés dans un dossier identifié « courrier indésirable ».

Les messages stockés dans le dossier « courrier indésirable » sont automatiquement supprimés au-delà d'un temps prédéfini (30 jours par défaut).

Pour des raisons de sécurité, l'envoi et la réception de courriel vers l'extérieur avec des pièces jointes constituées de fichiers exécutables sont bloquées par défaut (exemples : *.exe, *.scr, *.pif, *.asf, *.ade, *.adp, *.bas, *.bat, *.com, *.hlp, *.cmd, *.cpl, *.crt, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pcd, *.reg, *.sct, *.shb, *.shs, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh, *.cat, *.mov, *.adb, *.dbx, *.sht, *.cab, *.chm...).

Tous les courriels entrants et sortants sont analysés par un antivirus (virus, troyen, malware).

Celui-ci ne peut être garanti efficace à 100% et la vigilance doit rester de mise.

7 INTERNET

7.1 MOYENS D'ACCES

Les utilisateurs de l'INERIS disposent d'un accès à Internet au travers des ordinateurs connectés au réseau informatique de l'INERIS et/ou de moyens nomades (portables, ordiphones, etc.)

7.2 USAGES

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient. Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, à l'ordre public, ou au règlement et valeurs de l'INERIS, ne mettant pas en cause également l'intérêt et la réputation de l'institut, est admise.

7.3 ACCES WEB

Quel que soit le moyen d'accès ou l'usage, l'utilisateur doit respecter certaines règles.

La publication d'informations et de documents sur un support public entraîne une responsabilité personnelle de leur auteur devant la loi, que la responsabilité de l'institut en tant que personne morale ne saurait exonérer.

Il est rappelé que les employés ont accès à de nombreuses sources d'information plus ou moins contrôlées via internet et qu'une journalisation de ces accès est enregistrée et conservée comme précisé au paragraphe 7.5.

7.4 E-REPUTATION ET UTILISATION DES RESEAUX SOCIAUX

Les employés de l'INERIS bénéficient comme tous les citoyens d'un droit d'expression.

En application du principe de loyauté et du devoir de réserve auquel ils sont soumis, un employé ne doit pas compromettre la réputation de son employeur, donc de l'institut.

Cette obligation va au-delà des locaux dans lesquels les utilisateurs travaillent et au-delà de leurs horaires de travail.

Elle est permanente et s'applique de fait sur internet et en particulier sur les réseaux sociaux.

7.5 FILTRAGE ET REGLES DE TRAÇABILITE

La navigation sur internet est limitée par une solution de filtrage d'URL automatique qui interdit l'accès aux sites illicites proscrits par les dispositions légales et réglementaires.

Les catégories automatiquement bloquées par les systèmes de filtrage INERIS sont :

- Pédophilie, pornographie, sexualité, loisirs sexuels, nudité ;
- Violence, discrimination, haine raciale, révisionnisme, sexisme ;
- Jeux d'argent et paris en ligne, jeux en ligne et jeux vidéo ;
- Piratage et contournement des sécurités informatiques, peer-to-peer ;
- Substances addictives et illégales.

De plus, le filtrage des urls bénéficie également des traitements suivants pouvant conduire au blocage des flux :

- Antivirus web à partir de base de signatures multiples antivirus / anti-malware ;
- Filtrage par réputation web par évaluation du degré de confiance des URL.

Si un « dé-filtrage » sur un site précis est rendu nécessaire par l'activité professionnelle, il doit faire l'objet d'une validation hiérarchique et de l'accord du RSSI après évaluation du risque associé.

L'INERIS se réserve le droit de bloquer l'accès aux sites dont le contenu est jugé illégal, offensant ou sans rapport avec les missions de ses employés.

L'ensemble des connexions réalisées depuis un poste de l'INERIS bénéficie d'une traçabilité exhaustive, s'appuyant sur des outils dédiés uniquement accessibles aux administrateurs de la DSI.

Ces connexions génèrent des journaux d'activité (connexion, tentative, échec, déconnexion, etc.), protocole (tcp, udp, http, https, snmp, etc), @ IP, URL, heure, date, etc, dont le format est standardisé et sauvegardé sur des serveurs dédiés. Ils peuvent être audités ponctuellement, par exemple suite à un incident, ou dans le cadre de vérifications du respect de la charte.

Dans tous les cas, les contenus des transactions véhiculant des données personnelles ne sont pas analysés.

La journalisation de ces accès est enregistrée et conservée conformément à la réglementation.

À tout moment, seulement en réponse à une demande actée d'une autorité administrative ou judiciaire compétente, ces informations enregistrées peuvent être transmises.

8 LA SECURITE

8.1 LE MOT DE PASSE

L'authentification par votre nom d'utilisateur et votre mot de passe constitue l'unique moyen d'accéder à votre poste informatique, vos données et programmes nécessaires à l'accomplissement de vos missions.

A l'aide de votre mot de passe, un utilisateur mal intentionné peut avoir un accès illégitime à une session (envoyer des messages en au nom du titulaire, utiliser ses fichiers, accéder à des applications qui lui sont propres, etc...). C'est pourquoi chacun doit garder son mot de passe secret et ne le communiquer à quiconque. En particulier :

- Le mot de passe doit respecter la politique en vigueur au sein de l'institut : 8 caractères dont au moins 3 critères de complexité : majuscule, minuscule, chiffre, caractère spécial¹ ;
- Le support utilisateur est à votre disposition pour toute aide à la configuration de votre mot de passe ;
- Le mot de passe doit être connu de vous seul et doit être caché : ne le communiquez pas. Si vous pensez qu'un tiers en a eu connaissance, vous devez le changer immédiatement ;
- Si un collègue doit pouvoir accéder à certains de vos documents, assurez-vous de les enregistrer dans un dossier partagé sur l'espace prévu à cet effet ;
- Vous ne devez pas laisser votre mot de passe apparent (post-it ou autre support mis en évidence sur votre espace de travail) ;
- Vous ne devez pas composer votre mot de passe sous les yeux d'un tiers.

A noter :

- Assurez-vous qu'une mise en veille automatique avec mot de passe est effective sur votre poste ;
- En cas d'absence de courte durée, vous devez verrouiller votre session par la combinaison de touches « touche windows + L ».

Vous devez :

- Prendre toutes les précautions requises de sécurité lors du transit d'informations confidentielles au sein de l'institut ;
- Conserver votre mot de passe secret ;
- Alerter au plus vite le service support « SupplInfo » si vous pensez être victime d'une action ou tentative d'usurpation de votre compte ;
- N'utiliser que des progiciels mis à votre disposition par l'INERIS. Tout usage d'un autre logiciel engage votre responsabilité ;
- Utiliser les données numériques aux seules fins prévues.

¹ Caractère spécial : ~ ! @ # \$ % ^ & * _ - + = ` | \ () } { [] : ; " ' < > , . ?

Vous ne devez pas :

- Ouvrir des documents électroniques dont l'origine vous est inconnue ;
- Consulter ou diffuser des informations illégales, contraires à l'éthique de l'INERIS car vous engageriez votre responsabilité et risqueriez de porter atteinte à l'image de l'institut vis-à-vis de tiers ;
- Tenter d'accéder à des informations ou à des applications en dehors des droits qui vous sont normalement attribués. Si vous détectez une faille, signalez-la à SUPPINFO ;
- Laisser l'accès à votre environnement de travail à des personnes extérieures à l'institut ;
- Laisser ouvert en permanence votre accès Wifi et Bluetooth. Veiller à couper ces accès dès que vous n'en avez plus l'usage ;
- Utiliser ou essayer d'utiliser des comptes autres que le vôtre ou de masquer votre véritable identité ;
- Tenter de lire, modifier, copier ou détruire des données autres que celles auxquelles vous êtes censé accéder dans le cadre de vos missions professionnelles ;
- Quitter votre poste de travail sans vous déconnecter ou mettre l'écran en veille sécurisée.

8.2 RESPONSABILITE

Les accès frauduleux aux systèmes d'information (curiosité malsaine, vol d'informations, sabotage, modification ou divulgation de données, chantage, détournement, etc. ...) sont répréhensibles.

- ✓ Vous pouvez, en ne prenant pas les précautions prescrites, être involontairement complice d'une atteinte au fonctionnement du système ou d'une compromission d'informations sensibles et être sanctionné pénalement.
- ✓ Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau informatique sont analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.
- ✓ Dans le cadre de sa mission de protection du système d'information, d'engagement de sa responsabilité et de l'amélioration de sa productivité, l'INERIS enregistre la durée des connexions, les sites visités et les volumes téléchargés ainsi que toute activité relative à l'usage des serveurs, de la messagerie électronique, d'intranet et d'internet.
- ✓ Les administrateurs du système d'information disposent de privilèges d'accès pour accomplir leurs missions de maintenance et de gestion technique. Ces employés sont connus, limités en nombre, sensibilisés aux risques et tenus au secret professionnel.
- ✓ Les services informatiques de l'INERIS opèrent les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité en s'appuyant notamment sur les fichiers de journalisation.
- ✓ Le constat de toute utilisation illégale pourra donner lieu, après décision actée de l'autorité hiérarchique ou judiciaire, à la suppression des accès et/ou à des sanctions disciplinaires.
- ✓ Il est interdit aux employés de l'INERIS d'utiliser des connexions spéciales visant à dissimuler certaines de leurs activités, comme par exemple des VPN privés ou le réseau TOR.

Les employés de l'INERIS ne bénéficient pas du statut d'administrateur de leur poste de travail, pour des raisons de maîtrise des risques et afin de se prémunir de comportements déviants. Ainsi, l'installation de programmes ou d'applications à des fins professionnelles doit faire l'objet d'une demande validée par la hiérarchie directe de l'employé et la DSI.

Les applications dont l'usage n'est pas en adéquation avec un contexte professionnel sont strictement interdites sur les postes de l'institut à l'exception des dispositifs pour lesquels un usage mixte Professionnel/Personnel est configuré par la DSI.

9 LA TELEPHONIE

Les employés dont les missions ou les fonctions le nécessitent disposent d'un accès téléphonique professionnel vers l'extérieur.

Même si cet accès peut être limité à une zone géographique (locale, nationale ou internationale), l'usage que vous pouvez en faire est précisément encadré.

Veillez à maîtriser les informations que vous pouvez communiquer à l'extérieur et à vous assurer de l'identité de votre interlocuteur.

9.1 TELEPHONE PORTABLE PERSONNEL

L'usage de votre téléphone portable personnel sur le lieu de travail est toléré dans la mesure où cet usage est loyal, ponctuel, discret, de courte durée, et qu'il ne ralentit pas l'accomplissement des tâches qui vous sont confiées.

9.2 TELEPHONE PORTABLE PROFESSIONNEL

Certains des collaborateurs de l'INERIS sont dotés par l'INERIS d'appareils téléphoniques portables.

- ✓ Par courtoisie, pensez à activer le mode silencieux en réunion.
- ✓ Vous êtes responsable de votre forfait et vous devez veiller au bon respect des dépenses associées.
- ✓ Un bilan de consommation est périodiquement réalisé dans le but de contrôler l'utilisation du téléphone, les coûts associés et, ainsi, d'éviter les abus. Nominatif, ce rapport dresse l'inventaire par employé des coûts de téléphonie : consommation, SMS, MMS, numéros surtaxés, appels à l'étranger.
- ✓ Le directeur peut demander le détail des appels passés (sur les 6 premiers chiffres) et en cas d'abus prendre les mesures qui s'imposent.
- ✓ L'utilisation d'ordiphone (smartphone ou tablette) pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages et des données, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

10 DEVELOPPEMENT DURABLE

- **Economisez le papier et l'encre**
 - ✓ Privilégiez la numérisation ;
 - ✓ Utilisez la messagerie électronique pour les échanges de courriers internes voire externes ;
 - ✓ Privilégiez les impressions en noir et blanc, limiter l'usage de la couleur ;
 - ✓ Limitez les impressions ; privilégier la diffusion numérique et imprimer en recto-verso.
- **Economisez l'énergie électrique**
 - ✓ Arrêtez systématiquement votre ordinateur et ses périphériques en fin de journée ;
 - ✓ Veillez à réduire le volume des messages, des pièces jointes et des fichiers stockés.
- **Respectez les consignes de collecte sélective du papier ou des consommables informatiques** (corbeille à double compartiment...).

11 L'USAGE DES TERMINAUX PRIVES A DES FINS PROFESSIONNELLES

Le AVEC (Apportez Votre Equipement de Communication) ou BYOD (Bring Your Own Device) correspond à une pratique où les collaborateurs d'entreprise utilisent leurs équipements informatiques personnels à des fins professionnelles.

L'utilisation des terminaux personnels (PC, Smartphones, Tablettes...), à des fins professionnelles peut générer des difficultés en matière de sécurité des systèmes d'information (intégrité et confidentialité des données de l'institut).

En effet, l'utilisation du BYOD présente des menaces pour l'INERIS :

- Fuites d'informations confidentielles ;
- Vecteur d'infection par virus ;
- Accès non autorisé au réseau (intrusion frauduleuse) ;
- Engagement de la responsabilité civile de l'institut en tant que FAI (fournisseur d'accès internet) ;
- Perte d'informations.

Cette pratique, qui ne relève pas d'un droit individuel des employés, n'est pas autorisée à l'INERIS.

Les seuls modes autorisés de connexions au système d'information INERIS sont :

- La messagerie professionnelle accessible pour un utilisateur depuis un terminal externe via internet à la condition de disposer de droits et moyens de connexion validés par la DSI ;
- La connexion aux données du système d'information de l'INERIS via le dispositif de réseau VPN sécurisé depuis un terminal INERIS à la condition de disposer des droits et moyens de connexion VPN validés par la DSI. Tout autre mode de paramétrage est interdit.

L'institut dégage toute responsabilité en cas de survenue d'un incident de sécurité ayant pour origine l'utilisation par un salarié d'un outil informatique non professionnel.

12 ABSENCE PROLONGEE / DEPART DE L'INERIS

12.1 ABSENCE PROLONGEE

En cas d'absence prolongée prévue du bureau (plusieurs jours ouvrés consécutifs à convenir avec la hiérarchie), vous devez, via l'outil de messagerie, donner l'accès à l'un de vos collaborateurs ou émettre un message de réponse automatique indiquant à l'émetteur qui contacter : ceci vous évitera de bloquer de manière involontaire un processus de travail.

Vous devez également prendre toute disposition pour rendre accessibles les données et documents nécessaires au service.

Si les dispositions ci-dessus ne peuvent être prises et pour des raisons de continuité de service, les dossiers et courriels professionnels pourront être consultés. Cette autorisation de consultation ponctuelle du poste, de la messagerie ou de l'espace de travail doit faire l'objet d'une demande de la hiérarchie auprès de la DRH.

Au retour, l'utilisateur est informé de ces accès par un message de la hiérarchie.

12.2 DEPART DE L'INERIS

En cas de départ de l'INERIS, l'utilisateur doit se charger préalablement de mettre à disposition le contenu de sa messagerie et de ses dossiers de travail à son responsable hiérarchique.

Conformément aux procédures en vigueur, le compte informatique et la boîte aux lettres électronique pourront être définitivement et irrémédiablement supprimés après son départ.

L'utilisateur doit restituer aux services informatiques les matériels mis à sa disposition.

Le document de restitution de matériel est validé par le responsable hiérarchique conformément aux dispositions définies par le circuit départ.

12.3 CAS PARTICULIER D'UN DEPART SOUDAIN D'UN EMPLOYE

En cas de départ soudain d'un employé de l'INERIS, la boîte aux lettres restera accessible, au cas par cas, avec routage éventuel des courriels vers une adresse annexe, par transfert ou délégation, auprès du responsable hiérarchique, à toutes fins de continuité de service. Cet accès se fera en lecture, car l'utilisation pour envoi de courriel depuis une BAL clôturée est strictement proscrite.

Les accès au poste de travail et aux dossiers seront également transmis à la hiérarchie.

Les courriels et les dossiers identifiés comme « Personnel » tel que définis dans la présente charte ne seront en aucune manière accessibles à la hiérarchie et pourront être détruits par la DSI.

13 VIE PRIVEE / DROIT A LA DECONNEXION

L'INERIS veille au respect de la vie privée des utilisateurs et de son équilibre vis-à-vis des obligations professionnelles. Ceci concerne notamment :

- Le stockage des données et l'usage de la messagerie

Comme il est précisé dans les paragraphes précédents, en dehors d'une requête émanant d'une autorité judiciaire, les dossiers et les messages identifiés « Personnel » ne peuvent en aucune manière être communiqués à des tiers, quel que soit leur niveau hiérarchique.

- La géolocalisation

Les matériels mis à disposition des salariés (ordinateurs et ordiphones) sont paramétrés de façon à ne pas être géolocalisés par l'INERIS. Toutefois, l'INERIS pourra forcer ce paramétrage dans les cas suivants :

- En accord avec l'intéressé, par exemple pour le suivre dans des pays dangereux, en cas de perte ou de vol du matériel,
- En cas de situation d'urgence signifiée par écrit par la Direction Générale (par exemple attentat, situation de danger, ...)

L'utilisateur veillera à ne pas rendre volontairement impossible ce forçage en modifiant le paramétrage de son matériel.

- Le droit à la déconnexion

En dehors des modalités précisées dans le règlement intérieur concernant le temps de travail ou les astreintes, les salariés de l'INERIS n'ont pas l'obligation d'être joignables ou connectés aux systèmes d'informations de l'INERIS.

14 RESPONSABILITES - SANCTIONS

La loi, les textes réglementaires et cette charte définissent les droits et obligations des personnes utilisant les ressources informatiques et les services internet.

Les utilisateurs ne respectant pas les obligations définies dans la charte sont passibles de sanctions disciplinaires et, le cas échéant, sont passibles de sanctions pénales en cas d'affaire judiciaire affectant l'INERIS sur le champ des systèmes d'information.

Les responsables hiérarchiques ont pleine autorité pour prendre les mesures conservatoires nécessaires en cas de manquement à la présente charte et aux lois, et interdire aux utilisateurs fautifs l'accès aux ressources informatiques et/ou aux services internet, ces utilisateurs fautifs pouvant être présentés devant l'instance disciplinaire compétente.

Sous couvert de l'autorité hiérarchique compétente, les administrateurs du réseau se réservent le droit de prendre toutes mesures conservatoires, en cas d'urgence ou de manquements graves ou répétés aux règles de sécurité, afin de sauvegarder l'intégrité du réseau et des postes de travail de ses usagers.

14.1 CONTROLE ET AUDIT

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

Elles se justifient par les obligations incombant à l'INERIS et par un souci de sécurité et de bon fonctionnement des infrastructures du réseau informatique.

En effet, pour son activité, l'INERIS est en particulier soumis à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données et de la loi dite « Informatique et libertés ».

L'INERIS dispose également d'un pouvoir de contrôle de l'activité des utilisateurs et en particulier le respect par eux de la présente charte.

L'utilisation des moyens informatiques et de communication électronique pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser l'utilisation conforme ou encore de mener des analyses statistiques.

Ainsi, la DSI de l'INERIS doit :

- Vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne au travers de procédures de supervision de routine ;
- Contrôler l'origine licite des logiciels installés ;
- Conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- Transmettre sur requête aux autorités judiciaires tout ou partie des enregistrements disponibles.

En outre, à la demande de la Direction générale, la DSI pourra :

- Surveiller le contenu des informations qui transitent sur son système d'information ;
- Vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- Diligenter des audits d'usage des ressources et de contenu des informations pour vérifier que les consignes stipulées dans la présente Charte sont appliquées ;
- Procéder à toutes copies utiles pour faire valoir ses droits.

En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité de l'INERIS, la direction des systèmes d'information informe la Direction générale, puis, sur sa demande écrite transmet les traces individuelles des connexions incriminées.

En cas de non-respect avéré de la présente charte par un utilisateur, la direction des systèmes d'information en avertit le supérieur hiérarchique.

En fonction des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement, sans préjuger d'éventuelles sanctions disciplinaires.

Tout matériel installé illicitement sera supprimé ou désactivé par les intervenants de la direction des systèmes d'information dès le constat de leur présence sur le poste de travail.