Charte d'utilisation des moyens informatiques

Sommaire

Titre I - Statut de la Charte

Article 1 – Préambule

La charte a pour vocation d'exposer les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre dans l'utilisation du matériel et des systèmes informatiques, afin de pouvoir bénéficier des avancées technologiques mises à sa disposition, tout en assurant la protection de l'intégrité du groupe ALTRAN.

Article 2 – Définition

2.1 Moyens Informatiques ou systèmes d'information

Le terme « moyens informatiques » ou systèmes d'information désigne les moyens techniques de traitement de l'information en général et notamment le poste de travail, les périphériques, les équipements de télécommunication, le téléphone, les serveurs, les applications (messagerie, internet, intranet, ...).

Un poste de travail standard est un poste de travail préconisé par la direction des systèmes d'information et configuré selon le modèle de la direction des systèmes d'information (DSI).

2.2 Utilisateurs

Le terme utilisateur recouvre l'ensemble du personnel de l'entreprise, y compris les intérimaires et les stagiaires présents dans l'entreprise, et plus généralement, toute personne ayant une mission à accomplir nécessitant un accès aux systèmes d'information dans les locaux Altran d'une des entreprises du groupe ou hors des locaux (salariés d'entreprises extérieures mis à disposition, prestataires de services...).

2.3 Helpdesk

Le terme helpdesk est utilisé en référence au service en charge d'être le centre d'assistance, point de contact unique entre la DSI et les utilisateurs, dont l'objectif est de répondre aux demandes d'assistance émanant des utilisateurs des moyens informatiques du Groupe.
Les utilisateurs peuvent contacter le helpdesk à l'adresse suivante :

helpdesk.france@altran.com

Titre II – Utilisation

L'utilisation des moyens informatiques, informations, accès aux réseaux et services Internet est soumis au respect des règles énoncées dans la présente charte, la politique de sécurité des systèmes d'information (PSSI) et les lois en vigueur.

Le bon fonctionnement des systèmes d'information du groupe suppose le respect des dispositions législatives et règlementaires qui s'imposent afin de garantir la sécurité, la performance des traitements, la conservation des données professionnelles et la confidentialité des informations.

Article 3 – Principe de base

La présente charte est un code de bonne conduite fondé sur la politique de sécurité. Elle appelle à une attitude loyale, courtoise, responsable et respectueuse d'autrui dans l'intérêt du groupe, de ses clients et de ses utilisateurs.

L'utilisateur doit consacrer l'usage des moyens informatiques mis à sa disposition à son activité professionnelle. Un usage personnel raisonnable de ces moyens est toutefois admis pour répondre aux nécessités de la vie courante et familiale, dans les conditions énoncées ci-après.

Article 4 – Responsabilité

Chaque salarié est responsable de l'usage des moyens informatiques et des informations mis à sa disposition. Il s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes notamment sur le fonctionnement normal du réseau, sur l'intégrité des systèmes d'information, sur la sécurité des informations et sur l'image de marque du groupe Altran. Cette responsabilité s'entend quel que soit le mode d'accès, sur site ou à distance.

L'utilisation de ces moyens informatiques doit être rationnelle, conforme et loyale afin d'en éviter la saturation, le dysfonctionnement ou le détournement à des fins personnelles.

Article 5 – Utilisation personnelle

L'usage à des fins privées des moyens informatiques mis à la disposition du salarié, est toléré à condition que :

- cet usage soit occasionnel et raisonnable,
- n'entrave en rien la bonne conduite des affaires du groupe Altran,
- n'entrave pas la productivité,
- n'ait pas d'impact négatif sur l'image du groupe Altran,
- ne constitue pas une infraction aux présentes instructions.

Les dispositions légales, le règlement intérieur, les contrats de travail s'appliquent pleinement même lors d'un usage personnel.

L'utilisateur qui souhaite utiliser, à des fins privées, les moyens informatiques mis à sa disposition est tenu de l'indiquer clairement et explicitement par l'utilisation du terme « personnel » ou « privé ». Cette mention doit obligatoirement apparaître dans le nom des fichiers ou répertoires ou dans le sujet des messages concernés.

Toutes les informations qui ne sont pas clairement identifiées comme « personnel » ou « privé », sont considérées comme des informations professionnelles.

Article 6 – Assistance

En cas d'incident ou d'anomalies, les utilisateurs doivent se rapprocher du helpdesk qui effectue le premier diagnostic. Seul le helpdesk est habilité à réaliser et à suivre les opérations de dépannage.

L'utilisateur concerné est chargé d'assurer l'accès des intervenants à son matériel, d'organiser le rendez-vous avec l'intervenant et d'informer des résultats le helpdesk.

Article 7 – Consignes de sécurité

7.1 Sécurité des connexions et des accès

- Connexion réseau

Seuls des postes de travail standards peuvent être connectés au réseau du groupe Altran sans autorisation particulière. La connexion de matériel informatique autre (ordinateur non standard, équipement réseau, serveur, ...) est soumise à autorisation explicite de la DSI du groupe.

La connexion de matériel informatique au réseau d'un client est soumise à autorisation préalable et explicite de celui-ci en respectant ses consignes d'utilisation et de sécurité.

- Contrôle d'accès logique

Conditions d'accès :
Le contrôle d'accès aux moyens informatiques du groupe est lié à la possession d'un identifiant nominatif et unique ainsi que d'un mot de passe. Le mot de passe doit respecter les règles de sécurité en vigueur (complexité, longueur, cycle de vie).

Cet identifiant et mot de passe sont strictement personnels et ne doivent en aucun cas être communiqués, prêtés, écrits ou divulgués pour quelque raison que ce soit.

L'utilisateur ne doit pas usurper, emprunter ou obtenir l'identifiant et mot de passe d'autres utilisateurs. Il doit protéger l'accès à son poste de travail en verrouillant sa session lorsqu'il quitte son poste de travail.

Gestion des absences :
Afin d'assurer la poursuite de l'activité et le bon fonctionnement du service, en cas d'absence de l'utilisateur, l'administrateur pourra à titre exceptionnel et sous réserve de l'autorisation de la hiérarchie de l'utilisateur, avoir un accès provisoire aux données professionnelles de l'utilisateur. Ce dernier est alors obligatoirement informé de cet accès, au plus tard à son retour d'absence.

Selon la durée de son absence et afin de garantir la sécurité des systèmes d'information, l'utilisateur peut voir sa messagerie suspendue (absence supérieure à un mois), et peut être amené à restituer le matériel (absence supérieure à 3 mois) qui lui a été fourni par Altran.

Gestion des départs (rupture du contrat de travail) :
Lors de son départ d'ALTRAN, il appartient à l'utilisateur de s'assurer que tous les fichiers professionnels sont enregistrés sur le réseau et accessibles à son responsable. En cas de préavis non effectué, la restitution du matériel se fait dès la notification de la rupture.
Le répertoire « privé » ou « personnel » d'un utilisateur quittant Altran, s'il n'a pas été détruit par ce dernier, sera supprimé sans copie, ni prise de connaissance préalable du contenu par Altran sous réserve d'un contrôle réalisé dans les conditions prévues au Titre VI ci-après.

Le départ d'un utilisateur entraîne la fermeture immédiate des accès à sa boîte aux lettres et la suppression de la boite aux lettres dans un délai d'un mois, sauf décision contraire de l'autorité hiérarchique de l'utilisateur. Il est de la responsabilité de l'utilisateur de faire suivre ses messages à caractère personnel en communiquant sa nouvelle adresse à ses interlocuteurs.

Tous les messages arrivant dans la boîte nominative fermée d'un utilisateur seront refusés à l'entrée avec un message en retour à l'émetteur.

7.2 Sécurité des informations

- Documents de travail

Les documents électroniques de travail doivent être organisés, classés et répertoriés correctement afin de faciliter le partage s'il y a lieu, les sauvegardes et les impressions. Pour le partage de document, l'utilisateur doit utiliser les moyens informatiques mis à sa disposition.
Lors des impressions, l'utilisateur choisit une imprimante locale ou réseau qui garantisse la sécurité de ses éditions. L'utilisateur doit les récupérer immédiatement.

- Sauvegarde des données

La sauvegarde des données stockées sur les postes de travail et les portables est de la responsabilité de l'utilisateur. Les données ainsi sauvegardées sur périphériques externe doivent être stockées en lieu sûr.
La sauvegarde des données stockées sur les dossiers réseau individuels est de la responsabilité de la DSI. L'accès à ces dossiers est réservé à chaque utilisateur. Il est recommandé de conserver les informations professionnelles importantes dans ce dossier.
La sauvegarde des données partagées stockées sur les serveurs, baies disques et espaces réseaux du groupe est de la responsabilité de la DSI.

7.3 Sécurité des moyens informatiques

- Configuration matérielle et logicielle

La configuration du poste de travail ou des moyens informatiques ne peut être modifiée qu'en cas de nécessité professionnelle, avec accord de la DSI.

Toute installation de matériel ou logiciel complémentaire doit être effectuée sous contrôle de la DSI ou du client en respectant les consignes de sécurité.

Toute installation et utilisation de logiciels, d'informations et d'œuvres au format numérique sera faite en respectant le cadre légal et les contrats de licences.

- Restitution de matériel et de logiciel

Lors de la restitution de matériel ou logiciel à la DSI, les dossiers et informations du client doivent être préalablement sauvegardés et transmis au client par l'utilisateur. Toutes les données personnelles et les données clients doivent avoir été effacées par l'utilisateur avant la restitution du matériel.
La restitution des matériels informatiques doit avoir lieu dès la fin de la mission concernée et doit comprendre l'ensemble des éléments prêtés. La DSI effectue une vérification de conformité par rapport aux matériels et logiciels empruntés.
La fiche de prêt est signée par la DSI et l'utilisateur pour validation et confirmation du retour.

- Support amovibles

L'utilisateur doit utiliser les supports amovibles dans le respect de la présente charte.
En particulier la connexion de ces supports est sous la responsabilité de l'utilisateur qui doit se protéger de tout risque notamment de virus informatique.
Lorsque les supports amovibles sont utilisés à des fins de sauvegarde, leur stockage doit être sécurisé. L'utilisateur est responsable de ceux-ci notamment en cas de vol, perte ou altération.

- Protection du matériel et des informations

La protection du matériel et des informations contre le vol, la copie et la dégradation doit être assurée en permanence.

Les matériels portables doivent être attachés par un câble de sécurité ou rangés sous clé.

Le détenteur d'un matériel doit en permanence être en mesure de justifier de la propriété du matériel et des informations (sur demande des services de sécurité du client par exemple).

En cas de vol d'un matériel ou d'information, le détenteur doit

- déposer une plainte auprès des autorités,
- informer immédiatement la direction des systèmes d'information du groupe (via le helpdesk) et son manager.

Titre III – Bon usage

Article 8 – Utilisation de la messagerie

Dans le cadre de l'utilisation de la messagerie, l'utilisateur doit être sensible au fait que par défaut les informations transitent en clair sur internet. En cas de besoin spécifique client, l'utilisateur doit contacter la DSI pour identifier la solution à mettre en place.
Tout message non identifié par la mention « personnel » ou « privée » dans l'objet est considéré comme professionnel.

Pour éviter de saturer les systèmes, l'utilisateur doit éviter les envois itératifs, répétitifs ou en grand nombre. Par ailleurs, l'utilisateur s'assure du respect de :

- la législation en vigueur, notamment à l'égard des tiers,
- l'image de marque du groupe,
- l'identité des destinataires et de leur capacité à recevoir des messages,
- l'accord du management, s'il y a lieu, pour cet envoi.

L'utilisateur doit être vigilant vis-à-vis des messages dont l'expéditeur est inconnu ou qui contiennent des pièces jointes ou des liens vers des sites internet, et ne doit pas exécuter de programme, ouvrir de pièce jointe ou se connecter à des sites internet dont il n'est pas sûr de l'origine. En particulier ne doit pas communiquer de façon inconsidérée son adresse de messagerie afin de ne pas être victime de spam.

L'utilisateur ne doit pas :

- relayer des messages de fausse alerte,
- participer à des chaînes de messages,
- intercepter, modifier et transférer à d'autres personnes ni rendre publiques les communications qui ne lui sont pas adressées.

L'usage de la messagerie et des listes de diffusion par les institutions représentatives du personnel est toléré uniquement dans l'exercice légal de leurs activités et selon les modalités définies dans l'accord spécifique les concernant le cas échéant.

Article 9 – Logiciel de protection

La configuration des logiciels de protection contre les virus, les logiciels espions, les intrusions et autres attaques ne doit pas être modifiée. Toute contamination devra être immédiatement signalée à la direction des systèmes d'information du client et/ou du groupe Altran par le biais du helpdesk.

L'utilisation des moyens de cryptologie n'est possible que si elle est expressément permise ou imposée par Altran. L'utilisation de moyens de cryptologie autres que ceux autorisés par Altran est interdite.

Article 10 – Utilisation d'Internet

Il est du devoir de l'utilisateur de respecter les consignes suivantes :

- se connecter uniquement par l'intermédiaire des dispositifs mis en œuvre par la DSI,
- ne pas compromettre le bon fonctionnement des serveurs, des sites, des applications ou services auxquels il accède,
- ne pas participer à des jeux ou des paris en ligne,
- ne pas utiliser les services Internet à des fins malveillantes en rendant accessibles à des tiers des informations ou des données confidentielles ou contraires à la législation en vigueur,
- ne pas déposer, copier ou transmettre des informations sur tout type de serveur sur internet sans y être autorisé par les responsables habilités (propriétaires de l'information),
- ne pas autoriser les installations ou mises à jour de logiciels à partir de connexion internet non sécurisées.

L'attention des utilisateurs est attirée sur le fait que la plupart des sites internet qu'ils visitent gardent une trace de leur passage. Dans certains cas, ces sites identifient précisément la provenance du visiteur et son identité électronique (en l'occurrence, celle d'Altran lorsque les sites sont visités en utilisant l'accès internet Altran).

Article 11 – Utilisation des espaces de stockage

Des espaces de stockage sont mis à la disposition des utilisateurs sur les serveurs du groupe. Ces espaces comportent des zones personnelles et des zones partagées. Ces espaces sont réservés au stockage de documents professionnels. La taille d'espace disponible pour chaque zone de stockage est limitée.

L'utilisation doit :

- Respecter les limites de taille définies et régulièrement archiver les documents inutiles ou obsolètes,
- Ne pas utiliser les espaces communs à des fins personnelles ou privées.

Article 12 – Interdiction

D'une manière générale, sont strictement interdits :

- la diffusion d'informations *confidentielles* relatives au groupe Altran, à ses clients, à ses partenaires ou aux salariés, sauf si la conduite des affaires le requiert raisonnablement,
- la diffusion de messages politiques, racistes, ou de propagande,
- la diffusion, le stockage ou le téléchargement d'informations ou d'œuvres en infraction avec le droit d'auteur,
- l'accès ou le stockage de publications à caractère injurieux, diffamatoire, raciste, pornographique, de harcèlement sexuel/moral, ou tout autre contravention ou délit d'ordre pénal ou civil,
- l'atteinte à tout signe distinctif appartenant à des tiers, en particulier aux droits de marques, notoires ou non, à toute dénomination sociale, enseigne, nom commercial et nom de domaine,
- l'accès aux données personnelles d'une tierce personne sans l'autorisation de celle-ci,
- l'accès aux données communes ou partagées du groupe Altran sans l'autorisation des personnes habilitées,

- l'altération, la copie ou la suppression des informations appartenant à une tierce personne, au groupe Altran ou au client,
- la mise à disposition d'utilisateurs non autorisés d'un accès aux systèmes ou au réseau quel que soit le type de matériel employé.

Tout contrevenant à ces interdictions considérées comme substantielles engage sa responsabilité et en assume les entières conséquences légales et financières.

D'une manière générale, l'utilisateur doit prendre conscience que ces traitements non professionnels sollicitent inutilement les ressources des moyens informatiques, le plus souvent partagées.

Titre IV – Administrateurs

Article 13 – Rôle des administrateurs

Les administrateurs ont pour mission d'assurer le fonctionnement normal de la sécurité des systèmes d'information. Ils sont conduits par leur fonction même à avoir accès aux informations professionnelles ainsi qu'aux informations personnelles et privées relatives à l'utilisateur, y compris celle stockées sur le disque dur du poste de travail.

Article 14 – Obligation de discrétion et de confidentialité

Les administrateurs sont tenus à une obligation de discrétion et de confidentialité dans le cadre de leurs fonctions. Ainsi, ils ne peuvent exploiter les informations et données professionnelles et personnelles relatives à un utilisateur, qu'à des fins visant à garantir le bon fonctionnement et la sécurité des moyens informatiques du groupe.

Dans le cadre des procédures de contrôle prévues au Titre VI de la présente charte :

- l'administrateur peut communiquer à l'employeur toutes informations et données professionnelles relatives à un utilisateur;
- l'administrateur ne peut pas communiquer des informations et données identifiées « personnel » ou « privé », sauf en cas de risque ou évènement particulier de nature à porter atteinte à l'intérêt collectif de l'entreprise.

Titre V – Audit

Pour assurer le bon fonctionnement des moyens informatiques du groupe Altran, des audits permanents sont réalisés, dans le respect de la confidentialité et de la vie privée des utilisateurs. En particulier, les salariés sont informés qu'Altran met notamment en œuvre, sur les systèmes d'informations et de communications, les contrôles récurrents suivants :

- Ordinateur : inventaire de la configuration matérielle et logicielle, audit des ouvertures de session
- Réseau : audit du trafic réseau
- Internet : audit des sites visités et du trafic par utilisateur
- Internet : filtrage de l'accès aux sites illégaux ou présentant des risques de sécurité
- Messagerie électronique : traçabilité des objets et destinataires des messages par émetteur
- Fichiers : audit des taux d'utilisation des espaces de stockages personnels et communs

En cas de présomption basée sur des indices de violation de la charte ou d'une règle légale, des contrôles peuvent être opérés afin de vérifier le respect des dispositions de la présente charte et des règles légales. Ces contrôles sont effectués dans les conditions ci-après.

Il est précisé que ces audits pourront être amenés à s'appliquer à tout nouveau support d'information et de communication en lien avec les évolutions technologiques.

Article 15 – Contrôle de l'ordinateur, des moyens informatiques mobiles

Les utilisateurs sont informés que les fichiers contenus sur le disque dur et les moyens informatiques mobiles mis à leur disposition peuvent faire l'objet d'un contrôle.
Ce contrôle peut porter aussi bien sur les fichiers professionnels que personnels.

- Le contrôle des fichiers professionnels par l'employeur est libre.
- Le contrôle des fichiers répertoriés « personnel » ou « privé » ne peut intervenir qu'en présence de l'utilisateur qui peut se faire assister d'un représentant du personnel de son choix. La convocation de l'utilisateur peut intervenir par tout moyen. Dans l'hypothèse où l'utilisateur ne peut être présent, il peut se faire

représenter par un représentant du personnel. L'utilisateur ne peut pas s'opposer à ce contrôle.

- Par exception, en cas de risque ou événements particuliers de nature à porter atteinte à l'intérêt collectif de l'entreprise, l'ouverture des fichiers peut intervenir sans que l'utilisateur soit convoqué.

Article 16 - Contrôle de la messagerie électronique

Les utilisateurs sont informés que la messagerie électronique nominative ou partagée peut faire l'objet d'un contrôle en cas de litige interne ou externe sur l'utilisation qui en est faite.

- Le contrôle des messages professionnels par l'employeur est libre.
- Le contrôle des messages répertoriés "Personnel" ou "Privé" ne peut intervenir qu'en présence de l'utilisateur qui peut se faire assister d'un représentant du personnel de son choix. La convocation de l'utilisateur peut intervenir par tout moyen. Dans l'hypothèse où l'utilisateur ne peut être présent, il peut se faire représenter par un représentant du personnel. L'utilisateur ne peut pas s'opposer à ce contrôle.
- Par exception, en cas de risque ou événements particuliers de nature à porter atteinte à l'intérêt collectif de l'entreprise, l'ouverture de la messagerie peut intervenir sans que l'utilisateur soit convoqué.

Les utilisateurs sont informés que l'entreprise se réserve la faculté de solliciter une mesure d'instruction dans les conditions légales, pour obtenir copie du contenu des messages personnels, s'il existe un motif légitime pour ce faire.

Article 17 - Contrôle de l'usage d'Internet

L'entreprise se réserve le droit, d'effectuer des contrôles sur l'utilisation d'Internet à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection d'intrusion et d'utilisation contraire à l'ordre public et aux bonnes mœurs.

Ces contrôles peuvent être de nature quantitative pour mesurer le temps passé et qualitative pour identifier les sites consultés sans rapport avec les missions de l'utilisateur concerné.

Article 18 - Contrôle de l'usage du téléphone

Les utilisateurs sont informés que les temps passés en communication, de même que le caractère professionnel de celles-ci peuvent faire l'objet d'un contrôle au moyen d'un examen des relevés téléphoniques ou de la mise en place d'autocommutateurs (Equipement d'interconnexion des téléphones avec le réseau de téléphonie publique).

Titre VI - Respect des règles et sanctions

Les règles exposées dans la présente charte impliquent une attention particulière, leur non-respect notamment par un usage abusif, inapproprié ou dangereux, étant susceptible d'entraîner des sanctions disciplinaires, des poursuites civiles et/ou pénales conformément à la législation en vigueur en fonction de la gravité des faits reprochés et/ou de leurs conséquences sur le préjudice subi par le groupe Altran.

Le groupe Altran se réserve le droit de prendre toute mesure pratique dans le respect du cadre légal afin d'établir les responsabilités en cause et d'empêcher toute utilisation abusive, irrégulière ou illégale des systèmes.

Il est rappelé que les droits d'accès aux moyens informatiques ainsi que les conditions d'utilisation sont accordés à chaque utilisateur, en considération stricte des fonctions qu'il occupe.

L'utilisateur est informé que toute tentative de s'arroger des accès indus à des systèmes informatiques, toute manipulation technique déloyale ou divulgation d'informations préjudiciables à un tiers ou au groupe Altran, tout usage volontairement contraire aux règles internes ou aux lois constituent une faute pouvant entraîner des sanctions et engager sa responsabilité individuelle civile et pénale.

Titre VII - Archivage et droits d'accès

Les utilisateurs sont informés que l'usage qu'ils font des moyens informatiques et de communication mis à leur disposition peut donner lieu à un enregistrement et conservation de données qui les concernent.

A cet égard, il est précisé que :

- les traces de connexion internet sont enregistrées et archivées par Altran pendant une durée de 6 mois ;
- les traces d'utilisation de la téléphonie fixe sont enregistrées et archivées par Altran pendant une durée de 6 mois ;
- les traces de tout message électronique reçu ou envoyé peuvent être conservées par l'Entreprise pendant une durée maximale de 6 mois, à compter de la date d'émission ou de réception.

Au-delà, toutes les données sont détruites.

La conformité à la loi informatique et libertés au sein de groupe Altran est assurée par la désignation d'un Correspondant Informatique et Libertés (CIL).
Ce correspondant assure les fonctions de recensement et de mise à jour de la liste des traitements automatisés et veille à l'application de la loi informatique et libertés au sein du groupe Altran.

L'utilisateur a droit d'accès, de modification et de suppression des informations à caractère personnel le concernant conformément aux dispositions légales de la Loi Informatique et Libertés du 6 janvier 1978.

Il doit s'adresser à :

Altran Technologies - Contact CNIL
2 rue Paul Dautier - CS 90599
78457 Vélizy-Villacoublay
France

ou par courrier électronique à :

contact.cnil@altran.com

Titre VIII - Cycle de vie de la Charte

Article 19 - Comité de sécurité des systèmes d'information et correspondant CNIL (CSSI)

Le comité de sécurité des systèmes d'information (CSSI) est l'organe de gouvernance de la sécurité du système d'information. Il est composé de membres du comité exécutif et d'experts fonctionnels.

Il soutient l'application et la communication de la présente charte, en lien avec le Correspondant Informatique et Libertés.

Article 20 - Evolution

Le CSSI assure l'évolution régulière de la présente charte. Cette évolution doit respecter les lois en vigueur et soutenir les mutations du groupe Altran et de ses systèmes d'information. Elle doit également permettre de prendre en compte les suggestions et les contraintes des entités opérationnelles, lors du déploiement de la charte.

Le Correspondant Informatique et Libertés participe à l'évolution de la charte en tant que gardien de l'application de la loi informatique et libertés au sein d'Altran.

Titre IX – Entrée en vigueur et articulation avec le Règlement Intérieur

Article 21 - Publicité, dépôt, entrée en vigueur

Le texte de la présente Charte est annexé au règlement intérieur en vigueur et a été soumis à l'avis :

- des comités d'hygiène de sécurité et des conditions de travail pour les matières relevant de leur compétence ;
- du comité central d'entreprise.

Cette Charte a été communiquée, accompagnée de ces avis, à Monsieur l'Inspecteur du travail en date du 1er octobre 2014, déposé au secrétariat greffe du Conseil des Prud'hommes en date du 1er octobre 2014, et affichée à la même date.

Elle entrera en vigueur le 1er novembre 2014 et sera diffusée à l'ensemble du personnel Altran par une publication accessible par l'utilisateur et mise à disposition sur l'intranet d'Altran.

Article 22 – Modifications ultérieures

Toute modification ultérieure ou tout retrait de clause de cette Charte serait, conformément au code du travail, soumis à la même procédure, étant entendu que toute clause de la Charte qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à l'entreprise du fait de l'évolution de ces dernières, serait nulle de plein droit.

Fait à Vélizy-Villacoublay,
Le 1er octobre 2014

Le chef d'entreprise

INNOVATION MAKERS