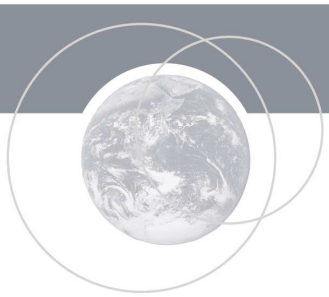
THALES



CHARTE RELATIVE AU BON USAGE DES RESSOURCES D'INFORMATION ET DE COMMUNICATION DANS LE GROUPE THALES

PREAMBULE

Les réseaux d'information et de communication proposent de nombreux services parmi lesquels certains sont de nature à apporter aux collaborateurs du groupe Thales une aide dans l'exercice de leurs activités professionnelles.

Chaque entreprise peut en effet être amenée à mettre à la disposition de ses collaborateurs des ressources appropriées lui permettant d'accéder à des services tels que notamment :

◊ Les applications bureautiques

◊ La messagerie électronique permettant d'échanger courriels et documents au niveau mondial

◊ Le site Thalesweb, sur lequel sont mises à disposition de l'ensemble des salariés des informations spécifiques sur le groupe Thales

◊ Les applications métiers et directions fonctionnelles, mises à disposition sur l'intranet, l'extranet ou l'internet.

◊ L'internet par lequel sont mises à dispositions, gratuitement ou non, des données numériques

Il importe néanmoins de souligner les risques inhérents à l'utilisation de ces ressources qui concernent notamment l'intégrité et la disponibilité des systèmes d'information du Groupe, la confidentialité des informations (notamment les données personnelles et les données réglementaires issues de la réglementation nationale ou internationale) et l'image des entreprises du Groupe Thales, qui peuvent être menacées par le mauvais usage, par le piratage du réseau ou des logiciels ou par l'introduction de virus.

C'est pourquoi, il est nécessaire que chaque utilisateur des ressources d'information et de communication au sein de l'une des entreprises du groupe Thales prenne pleinement conscience de ces risques, de la nécessité d'observer des règles de comportement permettant d'y faire face et de l'engagement de sa responsabilité personnelle en cas de non respect des règles figurant dans ce document.

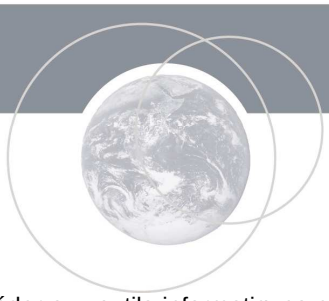
Les manquements à ces règles pourront être sanctionnés dans les conditions prévues par les règlements intérieurs des différentes entreprises du Groupe Thales.

CHAMP D'APPLICATION DE LA CHARTE :

Toute personne utilisant les ressources d'information et de communication de l'entreprise est soumise aux règles de cette présente Charte qui est complétée par des règles et procédures liées à la sécurité des systèmes d'information (disponible dans Chorus 2.0)

La Charte est mise à la disposition de l'ensemble des utilisateurs sur l'intranet du Groupe. Elle est systématiquement remise à tout nouvel arrivant.

L'autorisation d'accès aux ressources d'information et de communication, destinées à l'exercice d'activités professionnelles, est soumise à l'adhésion préalable de l'utilisateur à la présente Charte. Cette adhésion sera formalisée par la signature d'un document par l'utilisateur.



On désignera sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de Thales et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires ....

L'utilisation des ressources d'information et de communication dans l'entreprise est réservée à un usage professionnel, sauf exception pour répondre à une situation d'urgence. Ainsi, l'usage à titre privé de ces outils sera tolérée de façon limitée, à condition de ne pas perturber l'accomplissement de la mission du salarié et de ne pas porter atteinte à l'image du Groupe et au bon fonctionnement des systèmes d'information.

Article 1 : Engagements de l'entreprise

L'entreprise s'engage :

- à mettre en place les systèmes et outils permettant de garantir au mieux la sécurité globale des réseaux et des données, des applications et des accès aux postes de travail,

- à s'assurer du respect des procédures adaptées aux contraintes de la sécurité des ressources d'information et de communication : attribution des accès protégés aux nouveaux arrivants, extinction des droits des sortants, gestion des mots de passe…

Article 2 : Accès aux Ressources

L'accès aux ressources d'information et de communication du Groupe Thales est réservé au personnel Thales qui justifie d'un besoin validé par la hiérarchie.
Il ne peut être étendu au stagiaire et intérimaire que sous la responsabilité d'un personnel Thales dûment identifié.

L'accès aux ressources d'information et de communication du Groupe au personnel d'entreprises extérieures ou intervenantes dans les locaux fait l'objet, en cas de besoin, de dispositions particulières généralement définies dans le contrat commercial régissant leur relation.

L'autorisation d'accès aux ressources d'information et de communication est soumise à l'approbation de la hiérarchie de l'utilisateur et doit être formellement renouvelée en cas de changement de fonction ou de mutation.

Toute installation ou modification, matérielle ou logicielle (clé USB, lecteur de disque externe, lecteur multimédia, programmes, données de configuration…) doit se faire dans le respect des procédures de l'entreprise (notamment par l'Expression d'un Besoin Informatique ou une demande par e-catalogue).
Les administrateurs de serveurs, réseaux, systèmes sont considérés comme des utilisateurs et à ce titre sont également soumis aux règles définies par la présente Charte.
L'administrateur et le Responsable de la Sécurité des Systèmes d'Information (RSSI) ont un devoir impératif de confidentialité sur tout ce dont ils auront pu prendre connaissance dans l'exercice de leurs fonctions.

Article 3 : Sécurité des ressources d'information et de communication

L'usage des moyens fournis aux utilisateurs de Thales s'effectue à partir de comptes nominatifs dont l'utilisation est soumise à une séquence d'identification et d'authentification.

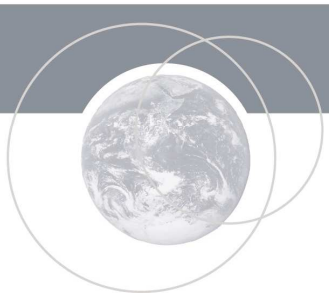
⇨ Tout possesseur d'un compte est responsable de l'utilisation de son identification d'utilisateur. Les moyens d'authentification (mot de passe, code pin, ..) sont personnels, confidentiels et incessibles.

L'utilisateur s'interdit l'utilisation de l'identifiant et du mot de passe d'un autre utilisateur.

En cas d'absence de l'utilisateur, des possibilités de reroutage du courrier électronique lui sont offertes sur une autre boîte aux lettres électronique du Groupe.

L'utilisateur est responsable de toute connexion aux ressources d'information et de communication effectuée à l'aide de son identifiant et de son mot de passe et de l'utilisation des données obtenues à partir des ressources d'information et de communication à l'aide de son identifiant et de son mot de passe.

A cet égard, il appartient à l'utilisateur d'utiliser tous les moyens mis à sa disposition par l'entreprise pour préserver la sécurité du système d'information et des données qu'il contient (logiciel anti-virus, procédure de sauvegardes…)



Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

-Signaler à son Responsable de la Sécurité des Systèmes d'Information (RSSI) toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement

-Ne jamais demander à un collègue ou à un collaborateur ses moyens d'identification/authentification

-Ne pas masquer sa véritable identité

-Ne pas usurper l'identité d'autrui

-Ne pas modifier le paramétrage du poste de travail

-Ne pas installer de logiciels sans autorisation

-Ne pas copier, modifier, détruire les logiciels propriétés de Thales

- S'assurer que son ordinateur se verrouille dès qu'il quitte son poste de travail

-Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas

-Ne pas copier de données professionnelles sur un support externe non fournis par Thales (fournisseur Thales) et ne pas envoyer d'informations professionnelles sur une messagerie personnelle.

Article 4 : Respect des obligations légales

Compte tenu des risques liés à l'utilisation des ressources d'information et de communication, l'utilisateur est soumis à des obligations particulières afin de protéger les biens informatiques et l'image du groupe Thales.

L'utilisateur est soumis au bon respect des dispositions légales ou réglementaires applicables en l'espèce et qui sanctionnent notamment le non-respect des bonnes mœurs, la diffusion de propos à caractère diffamatoire ou raciste, le piratage ou la fraude informatique, le non-respect du droit d'auteur, le non respect des dispositions de la loi « informatique et libertés »…

En matière de cryptologie, l'utilisateur, autorisé par le Groupe, devra veiller au respect des dispositions législatives nationales qui régissent l'usage, l'exportation et l'importation de ce type de systèmes.

Dans certaines activités du groupe Thales, le traitement, le stockage et la transmission d'informations classifiées défense (confidentiel défense et au-dessus) ou sensibles (diffusion restreinte et confidentiel spécifique) devront respecter des règles particulières obéissant aux contraintes réglementaires spécifiques.

Article 5 : Protection des intérêts du Groupe THALES

L'utilisation des ressources d'information et de communication doit se faire en respectant les règles sur la confidentialité des données manipulées en vue de garantir la préservation du patrimoine du groupe.

Dans ce cadre, l'instruction Thales intitulée « Protection des informations Groupe », relative à la classification des données selon leur niveau de sensibilité ainsi que les modalités de protection attachées à chaque type de document et de support devra être respectée. Cette instruction est notamment disponible sur l'intranet du Système d'information Groupe.

L'usage de la cryptologie est soumis à autorisation préalable de la Direction générale et doit être pratiqué dans le respect des règles nationales relatives à la cryptologie et des dispositions particulières de procédure définie par le Groupe.

Dans le cas de projets soumis à des contraintes spécifiques (partenariats, joint-venture…) des dispositions particulières de procédure devront être respectées.

Article 6 : Utilisation d'Internet

L'accès à l'Internet n'étant ni anonyme ni confidentiel, toute action menée est identifiable comme provenant du Groupe Thales.

Il appartient donc à chaque utilisateur d'être particulièrement discret lors de la publication ou la collecte d'informations, sur les activités du Groupe.

Les utilisateurs peuvent consulter les sites « Web » présentant un lien direct et nécessaire avec l'activité professionnelle.
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, aux bonnes mœurs et ne mettant pas en cause l'image et la réputation de l'entreprise, est tolérée si elle ne perturbe pas l'accomplissement de la mission des salariés ni la sécurité du réseau informatique du groupe Thales.
L'utilisateur ne doit pas tenter de pénétrer frauduleusement sur un site « Web » pour lequel il n'a pas d'autorisation d'accès.

L'utilisateur pourra participer à des media sociaux en rapport avec son activité professionnelle.
Tout utilisateur accédant à un tel media devra veiller à ne jamais divulguer d'information confidentielle sur Thales et sera responsable vis à vis du Groupe de toute atteinte à l'image de celui-ci qui résulterait des informations ou idées qu'il émet sur ce forum.

L'utilisateur pourra se référer à un guide des Médias sociaux élaboré par la Direction de la Communication Groupe.

Article 7 : Utilisation de la messagerie

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée à titre ponctuel et raisonnable et si elle ne perturbe pas l'accomplissement de la mission des salariés ni la sécurité du réseau informatique du groupe Thales.
Tout message figurant dans la messagerie professionnelle de l'utilisateur est présumé avoir un caractère professionnel.
Toutefois, le message qui comportera, dans son objet, la mention expresse ou manifeste de son caractère personnel ou privé bénéficiera du droit au respect de la vie privée et du secret des correspondances.

Ainsi, dans la limite des dispositions légales et jurisprudentielles applicables, Thales s'interdit d'accéder aux messages identifiés comme « personnel » ou « privé » dans l'objet de la messagerie du salarié,. La nature personnelle d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

Par ailleurs, Thales s'interdit d'accéder, en l'absence de l'utilisateur, aux documents enregistrés dans tout dossier identifié comme « personnel » ou « privé », dans la limite des dispositions légales et jurisprudentielles applicables.
Afin de participer à l'amélioration de l'usage de la messagerie électronique, la Charte pourra être complétée par des principes établis dans un Guide d'utilisation de la messagerie.

Tout message émis engageant son auteur, il convient d'utiliser la messagerie de manière opportune en s'interdisant tout message en « chaîne », alerte virale…, ou portant préjudice à l'entreprise ou à des tiers.

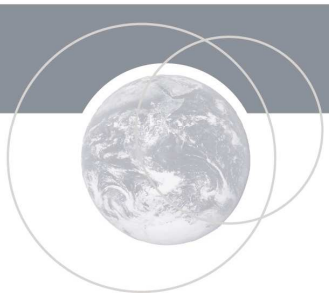
L'envoi de messages en diffusion générale est soumis à autorisation préalable du Chef d'Etablissement sur proposition de la hiérarchie.

Tout message, dès lors qu'il quitte l'entreprise, pouvant être intercepté, ne doit comporter aucune information susceptible de porter préjudice à l'entreprise ou à des tiers.
Tout message (entrant ou sortant) peut être soumis à un filtrage automatique permettant de vérifier que son contenu n'est pas de nature à porter préjudice à l'entreprise. En cas d'anomalies révélées par le filtrage, le message n'est pas diffusé et des informations complémentaires peuvent être demandées aux personnes concernées.
Afin de s'identifier clairement comme l'auteur du message, les courriers doivent être signés des nom et prénom de l'utilisateur.

L'usage de boites aux lettres internet à des fins professionnelles est interdit, car ces boîtes aux lettres ne sont pas protégées par Thales. En cas de besoin (personne travaillant sur site client, et ne disposant pas des outils de nomadisme), il est possible d'utiliser des boîtes aux lettres mises à disposition par Thales sur l'internet en « prénom.nom@mythalesgroup.com ».

Article 8 : Equipements nomades

On entend par « équipements nomades» tous les moyens techniques mobiles (ordinateur portable ou netbook dotés de la fonction mobility, tablette ou Smartphone équipés de push mail etc…) ou supports amovibles (clé USB etc.. ..).



- Un usage maîtrisé des outils d'information et de communication nomades :

Les possibilités de connexion à distance sont désormais multiples avec le développement des équipements nomades dotés des fonctions mobility ou push mail.
Ces évolutions présentent des avantages tant à titre professionnel que personnel.

Le groupe Thales considère toutefois que la mise à disposition de ces outils nomades doit s'accompagner d'une véritable vigilance de la part de l'entreprise et de la part de chaque utilisateur afin de s'assurer que l'équilibre entre la vie professionnelle et la vie privée est respecté.
Dans ce cadre, Thales s'engage à mettre en œuvre les mesures suivantes :
- S'assurer que la mise à disposition des salariés d'outils d'information et de communication nomades est nécessaire à la réalisation de leur mission et justifiée par la nature des tâches à accomplir et/ou le niveau de responsabilité du salarié.
- Remettre aux salariés, préalablement à toute mise à disposition d'un PC mobility ou d'un téléphone portable, une note de bonne utilisation de ces outils
- Former et sensibiliser l'ensemble des managers à la bonne utilisation des outils d'information et de communication nomades et notamment les bonnes pratiques relatives à l'utilisation de la messagerie électronique.

Par ailleurs, de façon à prévenir l'utilisation de la messagerie professionnelle ou du téléphone portable le soir, le week-end et pendant les congés, il est rappelé que (sauf situation exceptionnelle de décalage horaire) les outils nomades n'ont pas vocation à être utilisés pendant les périodes de repos du salarié.
A ce titre, les utilisateurs devront notamment veiller à n'envoyer des emails que pendant les heures normales de travail.

- Conditions de sécurité :

Quand cela est techniquement possible, les outils d'information et de communication nomades doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.
Quand un ordinateur portable se trouve dans le bureau d'un salarié qui en a l'usage, cet ordinateur doit être physiquement attaché à l'aide de l'antivol prévu à cet effet (sauf quand l'utilisateur est physiquement présent dans son bureau).
L'utilisation de téléphones portables pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, 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.

Article 9 : Contrôle

9.1. Moyens de contrôle interne :

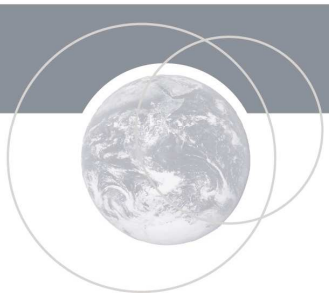
9.1.1.Filtrage automatique par mots clés et mise en quarantaine :

Les utilisateurs sont informés que le Groupe met en place, afin d'être à même de préserver ses intérêts, des moyens de filtrage automatique par mots clés avec mise en quarantaine automatique des messages et fichiers douteux (contenant certains mots clés par exemple « diffusion restreinte », « Thales Group Confidential », « pornographie ») ou de certaines natures (images, fichiers MP3..).

Les utilisateurs internes (émetteurs et destinataires) sont avisés de cette mise en quarantaine. A leur demande, le Responsable sécurité des services informatiques pourra analyser les messages et fichiers et les ré acheminer s'il ne détecte aucune anomalie au regard des règles déontologiques énoncés par la présente Charte. Sans action des utilisateurs internes les fichiers concernés seront automatiquement détruits dans le délai de quarante jours.

9.1.2. Détection et rejet automatique :

Seront rejetés automatiquement après détection :



- les virus et attaques logiques,
- les demandes de connexions sur certains sites,
- les intrusions détectées par la sonde d'analyse d'attaque réseau,
- les escroqueries véhiculées par les systèmes de messagerie (spam, phishing, etc…)
- les connexions des utilisateurs non dûment autorisés à franchir une passerelle inter-réseaux
- les modes de connexion fondés sur des protocoles interdits

9.1.3.Archivage :

9.1.3.1 Contenu :

A des fins de contrôle de sécurité, l'ensemble des flux d'informations pourra être archivé pendant six mois (à l'exception des flux entrants dans le Groupe qui compte tenu du secteur d'activité du Groupe et pour répondre à la demande des autorités de tutelle seront conservés deux ans).

Sont ainsi susceptibles d'être archivées les informations suivantes :

- L'ensemble des flux entrants ou sortants au niveau de nos passerelles inter-réseaux
- L'ensemble des fichiers journaux (qui contiennent notamment les tentatives de connexion, les comptes et sites accédés) et des fichiers systèmes
- L'ensemble des fichiers rapports constitués par les machines de sécurité (pare-feu, sonde de détection d'intrusion, anti-virus,…)

Toute diffusion d'information sur ces moyens, par des personnes non mandatées, est interdite tant à l'intérieur qu'à l'extérieur du Groupe.

9.1.3.2. Analyse et exploitation :

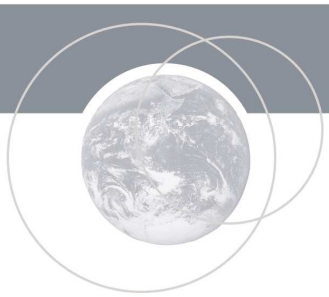
Le traitement d'informations et les moyens associés, déclarés à la CNIL, peuvent être utilisés à des fins de contrôle diligenté par la Direction générale, à partir des archives, des documents mis en quarantaine, et de l'état instantané du système d'information :

- sur demande des autorités (administratives, judiciaires ou de police..),
- en cas d'incidents divers (virus, intrusion, saturation des ressources, pannes)
- en cas d'acte de malveillance avéré ou constaté, ou de détournement des moyens ou des ressources d'information et de communication
- si nécessaire, à la demande du destinataire ou de l'émetteur.

9.2. Moyens de contrôle externe

Les utilisateurs sont informés que l'entreprise se réserve la possibilité d'effectuer des contrôles sur la teneur des informations déposées par les utilisateurs sur les forums Internet par consultation de serveurs Internet externes à l'entreprise et spécialisés dans des recherches de ce type.

Ces contrôles peuvent être opérés de façon inopinée ou systématique en cas d'incident ou d'acte de malveillance.



Article 10. Droit d'accès du salarié :

Dès lors qu'elles donneraient lieu à traitements, chaque salarié bénéficierait d'un droit d'accès aux données nominatives le concernant, et pourrait en demander, le cas échéant, la rectification.

Dans un tel cas, ce droit serait exercé par demande auprès du RSSI de l'entreprise.

Article 11. Protection des données à caractère personnel :

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués.

Thales a désigné un correspondant à la protection des données à caractère personnel chargé des traitements informatisés, en support aux processus Ressources Humaines du groupe. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.

Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le correspondant (coordonnées disponibles sur l'intranet)

Article 12. Entrée en vigueur de la charte :

La charte est entrée en vigueur suite à la déclaration à la CNIL n°759994 du 1er juin 2001 et aux consultations locales des Instances Représentatives du Personnel.

La mise à jour de la Charte entrée en vigueur en 2001, a fait l'objet d'une information du CCE de Thales le 29 juin 2012.