# Charte d'utilisation des ressources numériques

## Table des matières



## Préambule

Des moyens informatiques et des outils numériques (ci-après « les Ressources Numériques ») sont mis à la disposition des salariés, stagiaires, intérimaires, personnes de sociétés prestataires (ci-après les « Utilisateurs ») du Groupe Thales (ci-après le « Groupe ») afin de les aider dans l'exercice de leurs activités professionnelles.

L'utilisation de ces Ressources Numériques peut présenter des risques tels que ceux relatifs à l'indisponibilité des infrastructures, aux atteintes à la sécurité des systèmes d'information, la protection du patrimoine, notamment immatériel, du Groupe, son image, sa réputation, ou encore la non-conformité aux règlementations en vigueur applicables.

L'objet de la présente charte est de définir :

- les règles relatives aux usages permis des Ressources Numériques mises à la disposition des Utilisateurs,
- les règles de sécurité applicables,
- les mesures de contrôle mises en œuvre,

# 1. Champ d'application

La présente Charte d'utilisation des Ressources Numériques (ci-après la « Charte ») s'applique aux Utilisateurs autorisés à accéder et à utiliser les Ressources Numériques du Groupe.

Sont notamment considérés comme Ressources Numériques au sens du présent document :

- Le matériel informatique : ordinateurs, tablettes, téléphones, photocopieurs, périphériques ;
- Le réseau informatique : serveurs, routeurs, connectique ;
- Les applications bureautiques ;
- Les logiciels ;
- La messagerie électronique permettant d'échanger courriels et documents au niveau mondial ;
- Le site intranet « People Online » sur lequel sont notamment mises à disposition des informations spécifiques sur le Groupe ;
- Les applications métiers et directions fonctionnelles mises à disposition sur l'intranet, l'extranet ou l'internet ;
- Les outils collaboratifs, de communication à distance (audio conférence, vidéo conférence, etc.), y compris les outils et applications fournis par les tiers ;
- La messagerie instantanée.

# 2. Accès et utilisation des Ressources Numériques

L'accès aux Ressources Numériques du Groupe est réservé aux salariés du Groupe qui justifient un besoin validé par leur hiérarchie. Cet accès s'étend aux stagiaires et intérimaires sous la responsabilité d'un salarié Thales dûment identifié. Des dérogations particulières généralement définies dans le contrat peuvent autoriser l'accès à ces ressources au personnel d'entreprises extérieures ou intervenantes dans les locaux du Groupe.

L'autorisation d'accès aux Ressources Numériques doit être formellement renouvelée en cas de changement de fonction ou de mutation, tant du côté du service d'origine que du service d'accueil.

L'utilisation des Ressources Numériques dans le Groupe est réservée à un usage professionnel. Par conséquent, l'usage à titre privé de ces ressources est toléré à titre ponctuel et raisonnable, à condition de ne pas perturber l'accomplissement de la mission de l'Utilisateur et de ne pas porter atteinte à l'image du Groupe ou de ses entités et au bon fonctionnement des systèmes d'information.

A son départ, l'Utilisateur doit restituer l'ensemble des Ressources Numériques mises à sa disposition après avoir effacé ses fichiers, messages et données privés. En tout état de cause, les informations et données présentes sur les Ressources Numériques restituées sont supprimées dans un délai maximum d'un mois.

# 3. Messagerie électronique

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 Utilisateurs, ne porte pas atteinte à l'image et à la réputation du Groupe, ni la sécurité du réseau informatique du Groupe.

Tout message figurant dans la messagerie professionnelle de l'Utilisateur est présumé avoir un caractère professionnel.

Thales pourra ainsi accéder à la messagerie professionnelle de l'Utilisateur, y compris en son absence, dans les cas suivants :

- Afin de s'assurer du respect par l'utilisateur de l'ensemble des règles, chartes et politiques du Groupe Thales, en ce compris la Charte, ainsi que du respect de toute loi ou réglementation applicable au Groupe Thales ou à l'Utilisateur ;
- Afin de s'assurer de la continuité des activités du Groupe Thales et assurer le bon fonctionnement des équipements et systèmes informatiques du Groupe ;
- Afin d'empêcher, déterminer, examiner ou détecter des utilisations non autorisées des équipements, systèmes et ressources informatiques du Groupe pouvant impliquer le cas échéant une perte, destruction ou altération non autorisée ou illicite de données ;
- En cas d'incidents divers (virus, intrusion, saturation des ressources, pannes, acte de malveillance avéré ou constaté, etc) ou afin d'établir et maintenir la sécurité ou la sûreté des locaux, des équipements, des systèmes informatiques, actifs, appareils et données du Groupe ;
- Dans le cadre de procédures administratives ou judiciaires ainsi qu'en cas d'enquêtes internes ou d'audits ;
- A la demande d'une autorité compétente ;
- Si nécessaire, à la demande du destinataire ou de l'émetteur.

Tout message émis à l'extérieur du Groupe, pouvant être intercepté, ne doit comporter aucune information susceptible de porter préjudice au Groupe ou à des tiers.

**L'usage d'une messagerie privée à des fins professionnelles est prohibé**.

# 4. Internet

L'accès à l'Internet n'étant ni anonyme ni confidentiel, toute action menée à partir d'une Ressource Numérique fournie par le Groupe est identifiable comme provenant du Groupe Thales.

II appartient donc à chaque Utilisateur d'être particulièrement vigilant lors de la publication ou la collecte d'informations, en particulier des informations relatives aux activités du Groupe.

Les Utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle.

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 du Groupe, est tolérée si elle ne perturbe pas l'accomplissement de la mission des Utilisateurs ni la sécurité et le bon fonctionnement du réseau informatique du Groupe Thales.

Afin d'assurer la protection de son réseau, Thales définit une politique de filtrage des sites internet, procédant à une catégorisation de chaque site internet en fonction de son contenu, qui est mise en œuvre par les Responsables de la Sécurité des Systèmes d'Information du Groupe.

Cette politique tient compte:

- Du site internet demandé ;
- Du navigateur utilisé ;
- Du type d'action effectué ;
- Du contenu récupéré.

L'Utilisateur ne doit pas tenter de pénétrer frauduleusement sur un site internet pour lequel il n'a pas d'autorisation d'accès.

L'Utilisateur pourra utiliser des réseaux sociaux en rapport avec son activité professionnelle.

Tout Utilisateur accédant à un tel media devra veiller à ne jamais divulguer d'information confidentielle relative au Groupe Thales sauf autorisation expresse et préalable de la Direction 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 doit également se référer à l'espace intranet dédié à l'utilisation des réseaux sociaux élaboré par la Direction de la Communication Groupe.

Thales se réserve le droit d'analyser les données individuelles de connexion du salarié (sites visités, temps passé etc.).

# 5. Equipements nomades

On entend par « Equipements nomades » tous les moyens techniques mobiles (ordinateur portable doté de la fonction Mobility, tablette ou smartphone équipé de push mail etc.) ou supports de stockage amovibles (clef USB, NAS à connexion sans fil, etc.).

La mise à disposition de ces Equipements nomades doit s'accompagner d'une vigilance accrue de la part de chaque Utilisateur, notamment 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 :

- Remettre aux Utilisateurs, préalablement à toute mise à disposition d'un PC Mobility ou d'un téléphone portable, une note de bonne utilisation de ces Equipements nomades ;
- Former et sensibiliser l'ensemble des managers à la bonne utilisation des Equipements 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 Equipements nomades n'ont pas vocation à être utilisés pendant les périodes de repos de l'Utilisateur. Il est rappelé que les Utilisateurs disposent d'un droit à déconnexion en dehors des horaires d'ouverture de l'établissement dans lequel ils accomplissent régulièrement leur travail.

A ce titre, les Utilisateurs devront notamment veiller à n'envoyer des emails que pendant les heures normales de travail.

Quand un ordinateur portable se trouve dans le bureau d'un Utilisateur qui en a l'usage, il 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.

Lors des déplacements à l'étranger, des risques et des menaces supplémentaires peuvent peser sur la sécurité et la confidentialité des informations contenues dans les Equipements nomades. Une information complémentaire de la Direction de la sûreté Groupe pourra être communiquée à l'utilisateur en cas de besoin et des solutions techniques complémentaires pourront être mises en place.

# 6. Confidentialité et Sécurité

L'utilisation des Ressources Numériques doit se faire en respectant les règles sur la confidentialité des données traitées en vue, notamment, de garantir la préservation du patrimoine du Groupe. Elle doit en tout état de cause respecter l'instruction de gouvernance Protection des Informations Groupe.

L'usage des moyens fournis aux Utilisateurs du Groupe s'effectue à partir de comptes nominatifs dont l'utilisation est soumise à une séquence d'identification et d'authentification et à l'aide de mots de passe individuels respectant la Politique Groupe de Sécurité des Systèmes d'Information. Tout possesseur d'un compte est responsable de l'utilisation de son identification d'utilisateur. Les moyens d'authentifications (mot de passe, code pin, etc.) sont personnels et confidentiels.

L'Utilisateur est soumis au bon respect des dispositions légales ou réglementaires applicables 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 des droits de propriété intellectuelle et industrielle.

Il incombe à l'Utilisateur une utilisation raisonnée et responsable des Ressources Numériques mises à sa disposition.

L'Utilisateur est responsable, dans le respect de la réglementation applicable, de toute connexion aux Ressources Numériques effectuée à l'aide de son identifiant et de son mot de passe et de l'utilisation des données obtenues à partir des Ressources Numériques à l'aide de son identifiant et de son mot de passe ou de tout autre mode d'authentification mis à disposition (carte à puce, code PIN, double authentification, etc…).

Ainsi, il revient à l'Utilisateur d'utiliser tous les moyens mis à sa disposition pour préserver la sécurité du système d'information et des données qu'il contient.

L'Utilisateur s'engage à :

- Ne pas utiliser l'identifiant et le mot de passe d'un autre utilisateur ;
- Signaler à son Responsable de la Sécurité des Systèmes d'Information toute violation ou tentative de violation suspectée de son compte réseau et, de manière générale, tout dysfonctionnement et/ou faille de sécurité supposée ou avérée telle que tout courrier électronique reçu qui contiendrait manifestement une usurpation d'identité de personnes ou organismes à des fins d'escroquerie ou de vol d'information ;

- 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 tiers ou propriétés du Groupe dès lors que ces actions ne sont pas liées à la mission même de l'Utilisateur ;
- S'assurer que son ordinateur se verrouille dès qu'il quitte son poste de travail ;
- Ne pas accéder, ou tenter d'accéder à des informations pour lesquelles il ne disposerait pas d'autorisation d'accès ;
- Ne pas supprimer ou modifier des informations qui ne lui appartiennent pas
- Ne pas copier de données professionnelles sur un support externe non fourni par Thales ou un fournisseur agrée par Thales (y compris les plateformes de transfert de fichiers en cloud) ;
- Ne pas envoyer d'informations professionnelles sur une messagerie personnelle ;
- Ne pas utiliser de support informatique externe (exemple : clef USB, disque dur externe, etc.) sans validation préalable du Responsable de la Sécurité des Systèmes d'Information ou sans suivi de la procédure applicable aux stations blanches.
- Ne pas accéder aux Ressources Numériques dans des espaces ou transports publics (train, avion, restaurants, etc.) sans prendre les mesures nécessaires pour en protéger la confidentialité, la disponibilité et l'intégrité (par exemple par l'utilisation d'un filtre de confidentialité), et ce eu égard à la sensibilité des informations qu'elles contiennent.
- S'abstenir de traiter des informations de façon inadéquate compte tenu de leur degré de sensibilité (selon une classification légale ou interne au Groupe), lorsque le contexte ne permet pas d'en maintenir la confidentialité (par exemple : appel téléphonique depuis un lieu public).

# 7. Contrôle

## Filtrage automatique par mots-clefs et mise en quarantaine

Les Utilisateurs sont informés que le Groupe met en place, afin d'être à même d'assurer la sécurité de ses systèmes d'information et ainsi de préserver ses intérêts, des moyens de filtrage automatique par mots clés, catégorisation d'internet avec mise en quarantaine automatique des messages et fichiers douteux (contenant certains mots clés par exemple « diffusion restreinte », « Thales Group Confidential », « pornographie ») ou de certaine nature (images, fichiers MP3, etc.).

Les Utilisateurs (émetteurs et destinataires) sont avisés de cette mise en quarantaine. A leur demande, le Responsable de la Sécurité des Systèmes d'Information pourra analyser les messages et fichiers et les ré-acheminer s'il ne détecte aucune anomalie au regard des règles énoncées par la Charte. Sans action des Utilisateurs les fichiers concernés seront automatiquement détruits dans un délai de quarante jours.

## Messages et fichiers personnels ou privés

La mention expresse ou manifeste du caractère personnel ou privé du message ou du fichier permettra à celui-ci de bénéficier du droit au respect de la vie privée. Cette mention doit se trouver, pour un

message, dans son objet ou dans le nom du répertoire dans lequel il est stocké et, pour un fichier, dans son nom ou dans le nom du dossier dans lequel il est stocké.

Par conséquent, Thales s'interdit l'accès à ces messages et fichiers identifiés comme « privé » ou « personnel » sauf si :

- Elle dispose d'une autorisation judiciaire ou administrative à cette fin,
- Elle fait face à un risque ou un évènement particulier, tels que définis par la jurisprudence applicable.

## Détection et rejet automatique

Seront rejetés automatiquement après détection :

- les virus et attaques logiques,
- les demandes de connexions sur certains sites (par exemple : sites compromis, connus malveillant, délictueux... )
- 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 dument autorisés à franchir une passerelle inter-réseaux,
- les modes de connexion fondés sur des protocoles interdits.

## Archivage

A des fins de contrôle de sécurité, l'ensemble des flux d'informations pourra être archivé pendant une durée d'un an.

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.

## Analyse et exploitation

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

- sur demande des autorités administratives ou judiciaires,
- 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, de comportement contraires aux politiques de sécurité de l'entreprise,

- si nécessaire, à la demande du destinataire ou de l'émetteur.

# 8. Protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 telle qu'amendée relative à l'informatique, aux fichiers et aux libertés ainsi que le Règlement européen 2016/976 sur la protection des données à caractère personnel (RGPD) définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués.

Chaque Utilisateur bénéficie des droits suivants quant aux données personnelles (i.e., toute information se rapportant à une personne physique identifiée ou identifiable) traitées par le Groupe Thales et le concernant :

1. droit d'obtenir du responsable du traitement la confirmation que des données personnelles le concernant sont ou ne sont pas traitées et lorsqu'elles le sont, l'accès auxdites données personnelles, ainsi que les informations prévues par la réglementation applicable le concernant traitées par le Groupe Thales ;
2. droit d'obtenir du responsable du traitement (i) la rectification des données personnelles le concernant qui sont inexactes et (ii) que les données personnelles incomplètes soient complétées ;
3. droit d'obtenir du responsable du traitement l'effacement des données personnelles le concernant lorsque : (i) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectés ou traitées ; (ii) l'utilisateur retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ; (iii) l'utilisateur s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ; (iv) les données ont fait l'objet d'un traitement illicite ; ou (v) les données doivent être effacées pour respecter une obligation légale à laquelle le Groupe Thales est soumis ;
4. droit d'obtenir du responsable du traitement la limitation du traitement lorsque (i) l'exactitude des données est contestée par l'Utilisateur, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données ; (ii) le traitement est illicite et l'Utilisateur s'oppose à leur effacement et exige à la place la limitation de leur utilisation ; (iii) le responsable du traitement n'a plus besoin des données aux fins du traitement mais celles-ci sont encore nécessaires à l'utilisateur pour la constatation, l'exercice ou la défense de droits en justice ; ou (iv) l'Utilisateur s'est opposé au traitement pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de l'utilisateur
5. droit de préciser des directives relatives au sort de ses données personnelles après sa mort ;
6. droit de recevoir les données personnelles le concernant que l'Utilisateur a fourni au responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine si le traitement est effectué à l'aide de procédés automatisés et est fondé sur le consentement de l'utilisateur ou sur un contrat auquel l'Utilisateur est partie ;
7. droit de ne pas faire l'objet d'une prise de d'une décision fondée exclusivement sur un traitement automatisée (y compris le profilage) produisant des effets juridiques le concernant ou l'affectant de manière significative de façon similaire.

Le Correspondant Données Personnelles de la direction des Ressources Humaines veille au respect des droits des personnes (droit d'accès, de rectification, d'opposition, etc.). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le Correspondant

susmentionné à l'adresse dataprotectionrh@thalesgroup.com ou le Délégué à la Protection des Données personnelles du Groupe (DPD Groupe) à l'adresse : dataprotection@thalesgroup.com

## 9. Sanctions

Les manquements aux règles établies dans cette Charte pourront être sanctionnés dans les conditions prévues par les règlements intérieurs des différentes entités du Groupe Thales auxquels elle est annexée.

## 10. Accessibilité et entrée en vigueur

La Charte est mise à disposition de l'ensemble des Utilisateurs sur l'intranet du Groupe. Elle est, par ailleurs, systématiquement remise à tout nouvel arrivant. La Charte entrera en vigueur à l'issue des processus sociaux et mesures de publicité prévus par les dispositions légales.