AIRBUS

Information Management & Utilisation des Moyens du système d'information et technologies (IS&T) d'Airbus – 01/01/2019

1. OBJET & DOMAINE D'APPLICATION

1.1 Le présent Document a pour but d'informer les Utilisateurs des règles applicables à l'utilisation des Moyens IS&T (systèmes et technologies de l'information).

1.2 Les règles contenues dans ce Document s'appliquent indépendamment du fait que l'Utilisateur a recours aux Moyens IS&T sur des sites Airbus ou à l'extérieur.

1.3 L'objectif de ces règles est de garantir la confidentialité, l'intégrité et la disponibilité de toutes les opérations et de tous les intérêts d'Airbus. Conformément à cet objectif, le Département Sécurité d'Airbus est en droit de suivre et de contrôler l'utilisation des Moyens IS&T par tous les Utilisateurs.

2. UTILISATION DES MOYENS IS&T

2.1 Utilisation d'ordre général

2.1.1 Les Utilisateurs sont autorisés à exploiter les Moyens IS&T dans le cadre de leurs tâches professionnelles, à condition que cette utilisation respecte les dispositions de sécurité et les normes d'éthique décrites dans les présentes et complétées par des règles internes supplémentaires.

2.1.2 Ce Document est communiqué à l'ensemble des Utilisateurs.

2.1.3 Pour permettre la coordination des actions immédiates, tout risque d'atteinte à la sécurité (y compris mais sans s'y limiter : e-mails de phishing, infection par virus, perte ou corruption de données, vol de matériel, utilisation frauduleuse d'un compte utilisateur, accès non autorisé aux données ou transmission de contenu offensant) devra être immédiatement signalé au responsable local du département Sécurité d'Airbus.

2.1.4 Les Utilisateurs reconnaissent que toutes les activités menées sur une adresse e-mail d'Airbus ou via le réseau Airbus pourraient être interprétées par des personnes extérieures comme des actions d'Airbus. Par conséquent, toute activité réalisée par les Utilisateurs à l'aide des Moyens IS&T peut avoir un impact sur Airbus.

2.1.5 Des règles supplémentaires pourront s'appliquer à l'utilisation des Moyens IS&T pour des programmes militaires/de défense et/ou des éléments contrôlés à l'exportation (export control).

2.2 Utilisation Privée

2.2.1 L'utilisation des Moyens IS&T à des fins privées est expressément interdite, sauf dans les cas prévus par l'Article 2.2.2.

2.2.2 Toutefois, une utilisation occasionnelle des Moyens IS&T à des fins privées, pour contacter ses proches et effectuer des tâches quotidiennes, est tolérée uniquement dans les entités Airbus situées dans des pays où les lois nationales l'autorisent. Une telle utilisation des Moyens IS&T devra :

2.2.2.1 être conforme à la loi et ne pas être contraire aux intérêts et règlements internes d'Airbus ;

2.2.2.2 respecter la sécurité et l'intégrité des Moyens IS&T ;

2.2.2.3 demeurer raisonnable, brève et occasionnelle ; et

2.2.2.4 ne pas gêner ni entraver les performances ou les responsabilités professionnelles de l'Utilisateur.

2.2.3 Tout contenu accessible via, transmis par, ou enregistré sur les Moyens IS&T est considéré comme étant de nature professionnelle, sauf si ce contenu est clairement identifié comme étant « Privé » ou « Personnel » (dénommé ci-après « Données Privées»).

2.2.4 Toutes les Données privées devront être enregistrées par les Utilisateurs dans leur dossier « Privé » ou « Personnel ». Un dossier « Mes documents », ou tout autre « répertoire personnel », n'est pas considéré comme des Données privées, sauf s'il porte la mention spécifique « Privé » ou « Personnel ».

2.2.5 Les Utilisateurs sont responsables de la gestion de leurs Données privées. Airbus ne sera pas tenu responsable en cas de perte, de destruction ou d'interception illégale par un tiers de Données privées transmises ou enregistrées sur les Moyens IS&T.

2.2.6 Il incombe à l'Utilisateur de supprimer toutes ses Données privées des Moyens IS&T avant de renvoyer un appareil à Airbus pour quelque raison que ce soit. Airbus ne sera pas tenu responsable des dommages directs ou indirects résultant du fait que l'Utilisateur n'a pas supprimé ses Données privées sur les Moyens IS&T au terme de sa mission/son contrat de travail.

2.2.7 Si un Utilisateur découvre qu'il a accès aux Données personnelles d'un autre Utilisateur, il doit immédiatement contacter son DPO (Data Protection Officer) local.

2.3 Activités générales interdites

2.3.1 Il est expressément interdit aux Utilisateurs d'exploiter les Moyens IS&T pour exercer :

2.3.1.1 toute activité illégale ;

2.3.1.2 toute activité contraire aux intérêts d'Airbus ;

2.3.1.3 toute activité visant à promouvoir les activités commerciales d'un tiers ; et

2.3.1.4 toute activité visant à promouvoir les activités commerciales externes de l'Utilisateur.

2.3.2 Les Utilisateurs ne devront pas exercer d'activités nuisant ou susceptibles de nuire aux opérations, aux intérêts, à la réputation et aux relations d'Airbus, des clients d'Airbus et des partenaires commerciaux d'Airbus.

2.3.3 Les Utilisateurs ne devront pas détériorer ou affecter les intérêts ou la vie privée de tiers via les Moyens IS&T.

2.3.4 En outre, sont expressément interdites aux Utilisateurs les activités suivantes (liste non exhaustive) :

2.3.4.1 Autoriser des personnes étrangères au Département IM à accéder aux Moyens IS&T à des fins de maintenance et/ou de configuration ;

2.3.4.2 Partager leurs mots de passe et codes d'accès personnels ou tenter d'obtenir les mots de passe ou codes d'accès d'autres Utilisateurs, y compris de membres du Département IM ;

2.3.4.3 Contourner les étapes d'authentification d'Utilisateur ou de tout autre mécanisme de sécurité des Moyens IS&T ;

2.3.4.4 Utiliser et/ou installer des logiciels et/ou toute application non fournis par Airbus ou sans autorisation d'Airbus ;

2.3.4.5 Désactiver les programmes anti-virus ou tout autre logiciel de protection installé par le Département IM ;

2.3.4.6 Enregistrer, supprimer, copier ou dupliquer à des fins personnelles des informations, données ou logiciels appartenant à Airbus sans son autorisation préalable ;

2.3.4.7 Commettre des infractions aux règles de sécurité ou perturber les communications réseau (on entend par infraction aux règles de sécurité, notamment, l'accès à des données dont l'Utilisateur n'est pas le destinataire, la connexion à un serveur ou à un compte auquel l'Utilisateur n'est pas expressément autorisé à accéder) ;

2.3.4.8 Introduire des programmes et/ou des applications malveillants dans les Moyens IS&T (par ex. virus, vers, Chevaux de Troie, bombes e-mail, etc.) ;

2.3.4.9 Installer ou connecter à une infrastructure et/ou un réseau Airbus, tout dispositif électronique non autorisé (sans fil ou câbles, passerelles, ponts, dispositifs Internet 4G) susceptibles d'affecter le fonctionnement du réseau et de générer des risques d'accès non autorisés ; et

2.3.4.10 Modifier de quelque manière que ce soit la configuration des Moyens IS&T sans l'autorisation préalable d'Airbus fournie par le Département IM.

3. COURRIER ELECTRONIQUE

3.1 Les comptes de messagerie Airbus sont réservés à un usage exclusivement professionnel. Sous réserve des dispositions de l'Article 2.2.3, tous les e-mails transmis et/ou reçus sur des comptes de messagerie Airbus sont considérés comme des documents officiels détenus par l'entreprise, qui devront donc être soumis aux règles d'Airbus en matière de protection et de classification des informations.

3.2 L'utilisation privée occasionnelle des e-mails pour contacter ses proches et effectuer des tâches quotidiennes est tolérée, à condition qu'elle n'affecte pas le trafic normal des e-mails professionnels et qu'elle respecte les dispositions de l'Article 2 des présentes ainsi que les autres exigences et limitations en vigueur, telles qu'elles peuvent être énoncées dans le présent Document.

3.3 Les mesures et restrictions suivantes s'appliqueront à l'utilisation des e-mails :

3.3.1 Afin de détecter et d'éviter les menaces telles que notamment virus, chevaux de Troie, vers, spams malveillants et messages de phishing/vishing, le contenu de tous les e-mails des Utilisateurs sera filtré par Airbus. Nonobstant ces mesures de filtrage, en cas de réception d'un e-mail suspect, l'Utilisateur ne devra pas ouvrir les pièces jointes ou les liens qu'il contient, ni transmettre cet e-mail à un autre Utilisateur. Dans ce cas, l'Utilisateur devra signaler dans les meilleurs délais tout e-mail suspect reçu au département Sécurité d'Airbus.

3.3.2 L'Utilisateur devra transmettre toute information stratégique ou sensible conformément à la directive d'Airbus « Security Requirements for Company Data Classification and Protection (Exigences de sécurité pour la classification et la protection des informations de l'Entreprise) » (A1044).

3.4 Dans tous les cas, il est interdit aux Utilisateurs (liste non exhaustive) :

3.4.1 De solliciter, créer ou diffuser du matériel non professionnel, tels que chaînes de lettres, photos, fichiers vidéo ou audio, blagues, messages non sollicités, courrier indésirable ou autres messages de nature publicitaire, à l'intérieur comme à l'extérieur d'Airbus ;

3.4.2 De manipuler des e-mails à des fins non autorisées, par exemple en contrefaisant les informations d'en-têtes d'e-mails, ou en modifiant ou supprimant le pied de page des messages sortants ;

3.4.3 D'utiliser les listes de diffusion d'Airbus à des fins non professionnelles ;

3.4.4 D'ouvrir, enregistrer ou exécuter une pièce jointe d'un e-mail, excepté si cette pièce jointe est réputée fiable ;

3.4.5 De cliquer sur les hyperliens qui établissent une connexion vers des sites web inconnus ;

3.4.6 De divulguer des informations telles qu'identifiants de connexion et mots de passe, qui permettraient au destinataire d'accéder illégalement aux Moyens IS&T ;

3.4.7 De publier des adresses e-mail d'Airbus sur des sites web publics, entraînant ainsi l'ajout de ces adresses à des listes de diffusion de spams ou de mailing de masse ;

3.4.8 Les utilisateurs ne devront en aucun cas transmettre des e-mails et des pièces jointes d'ordre professionnel vers leurs dispositifs de stockage privés, y compris, mais sans s'y limiter, vers leurs comptes de messagerie privés, leurs comptes de cloud privés ou leurs dispositifs de stockage privés.

3.5 L'Utilisateur disposant d'un accès au compte d'un autre Utilisateur à des fins spécifiques conformément à la politique d'Airbus (« Accès autorisé spécifique ») devra satisfaire aux exigences suivantes :

3.5.1 L'Accès autorisé spécifique devra faire l'objet d'un accord écrit de l'Utilisateur dont le compte est consulté ; et

3.5.2 L'Accès autorisé spécifique devra être octroyé pour une durée définie.

3.6 En cas d'absence ou de départ imprévu d'un Utilisateur, il peut lui être impossible de fournir l'autorisation écrite prévue à l'Article 3.5.1. Dans ce cas, Airbus évaluera l'urgence du besoin d'accéder au compte et, s'il le juge nécessaire, autorisera une personne spécifique à accéder au compte e-mail de l'Utilisateur absent sous la supervision du DPO/Département HR. Cet accès sera autorisé uniquement s'il est conforme à la législation locale en vigueur. Les stagiaires et les sous-traitants/contractants d'Airbus ne pourront en aucun cas accéder aux comptes de messagerie des employés d'Airbus.

3.7 Dès l'annulation d'un compte de messagerie par Airbus, tous les e-mails envoyés à ce compte seront transférés à une personne désignée selon les procédures locales, afin d'assurer la continuité de l'activité.

4. INTERNET/INTRANET

4.1 L'accès à Internet/l'Intranet via les Moyens IS&T, y compris à distance, est autorisé pour un usage exclusivement professionnel.

4.2 L'utilisation privée occasionnelle d'Internet/de l'Intranet via les Moyens IS&T est autorisée pour contacter ses proches et effectuer des tâches quotidiennes, à condition qu'elle n'affecte pas le fonctionnement normal d'Internet/de l'Intranet et qu'elle respecte les dispositions de l'Article 2 du présent Document, ainsi que les autres exigences et limitations en vigueur, telles qu'énoncées dans les présentes.

4.3 Toutes les connexions à Internet/l'Intranet via les Moyens IS&T seront établies via les services standard d'Airbus (accès Internet, accès à distance).

4.4 Dans tous les cas, il est interdit aux Utilisateurs d'exploiter les Moyens IS&T pour (liste non exhaustive) :

4.4.1 Télécharger et stocker des fichiers, programmes, codes ou logiciels provenant de sources Internet non fiables sans l'autorisation préalable du Département Sécurité d'Airbus ;

4.4.2 Télécharger, stocker, installer, désinstaller, actualiser, utiliser ou distribuer des logiciels autres que ceux fournis ou autorisés par Airbus ;

4.4.3 Télécharger, stocker ou diffuser du matériel non professionnel ;

4.4.4 Télécharger, stocker ou diffuser du matériel non autorisé, protégé par un copyright et appartenant à un tiers ;

4.4.5 Consulter et utiliser des programmes de partage de fichiers « peer-to-peer » (par ex., programme Torrent) ;

4.4.6 Utiliser les services de messagerie instantanée à des fins professionnelles sans autorisation d'Airbus ;

4.4.7 Créer des sites web ou des blogs indépendants sur Internet. Toutes les informations de l'entreprise seront publiées sur le site web officiel d'Airbus : www.airbus.com ou équivalent et géré par le Département Communications d'Airbus ;

4.5 Il est expressément interdit aux Utilisateurs d'exploiter les Moyens IS&T pour accéder au contenu suivant :

4.5.1 Contenu pornographique/pédophile/obscène ;

4.5.2 Contenu raciste/sexiste, abusif ou humiliant, y compris les discours haineux et les publications dont le contenu prône la répression de certains groupes et individus, notamment, les minorités raciales/religieuses/de genre/sexuelles/d'âge/handicapées ;

4.5.3 Contenu potentiellement insultant ou diffamatoire ;

4.5.4 Contenu dégradant et/ou discriminatoire ;

4.5.5 Contenu relatif à l'obtention, la revente ou la consommation de drogues ;

4.5.6 Contenu faisant la promotion du ou incitant au terrorisme ;

4.5.7 Contenu relatif à l'exécution ou la promotion d'activités criminelles, telles que des instructions ou des références à des méthodes/procédures pour commettre des actes illégaux ;

4.5.8 Contenu relatif à l'occulte : publication d'opinions extrémistes sur l'occultisme, le satanisme ou autres sujets similaires ;

4.5.9 Réseaux anonymes (tels que TOR) ou utilisation de services VPN autres que ceux utilisés et autorisés par Airbus ;

4.5.10 Jeux (par ex., jeux vidéo, jeux en ligne, jeux d'argent, loteries, etc.) et marchés (par ex., eBay) ; et

4.5.11 Contenu de tout réseau social privé ou de comptes de messagerie privées à des fins professionnelles sans autorisation d'Airbus.

4.6 Il est expressément interdit aux Utilisateurs d'exploiter Internet/l'Intranet aux fins suivantes :

4.6.1 Exposer Airbus à des sanctions ou des situations embarrassantes ;

4.6.2 Stocker des informations Airbus sur un cloud public ou un service de stockage Internet privé (par ex., Dropbox, iCloud ou un serveur personnel), excepté si cette méthode de stockage a été formellement autorisée par le Département Sécurité d'Airbus ;

4.6.3 Divulguer des informations sur Airbus ou faire référence à Airbus sur des sites web publics, des chats, des forums, des blogs, des réseaux

sociaux ou tout autre média, sauf autorisation expresse du Département Communications d'Airbus.

5. MOYENS IS&T MOBILES

5.1 Airbus pourra fournir des appareils IS&T, tels que smartphones, tablettes, PC, etc., aux Utilisateurs (notamment via les modèles COD (Company Owned Device) ou CYOD (Choose Your Own Device)) pour leur permettre d'accéder au réseau Airbus à des fins professionnelles et conformément à l'Article 8.

5.2 Sous certaines conditions, les Utilisateurs pourront convenir d'utiliser leurs appareils mobiles privés à des fins professionnelles (à savoir, via le modèle BYOD (Bring Your Own Device)). Dans ces circonstances, l'utilisateur reste responsable des coûts dus à l'opérateur sollicité pour la fourniture des services mobiles. Si cette option est sélectionnée, Airbus installera les applications professionnelles nécessaires pour accéder au réseau Airbus. Ces applications professionnelles seront totalement isolées des applications personnelles/privées de l'Utilisateur et placées dans un conteneur strictement professionnel qui sera soumis à une Surveillance conformément à l'Article 8.

5.3 La navigation sur Internet via le réseau Wi-Fi d'Airbus sera filtrée et surveillée conformément à l'Article 8.

6. CONFIDENTIALITE

6.1 Les Utilisateurs traiteront toutes les informations en tant qu'informations confidentielles, y compris les faits, les questions, les documents et toute autre donnée obtenue dans le cadre de l'exercice de leurs fonctions professionnelles chez Airbus. Lesdites informations confidentielles demeureront la propriété d'Airbus, de ses clients et/ou de ses fournisseurs (le cas échéant). Cette obligation de confidentialité se poursuivra après la cessation ou la conclusion des activités de l'Utilisateur avec Airbus, conformément à la législation locale, au cadre contractuel ou aux autres règlements en vigueur.

6.2 Les Utilisateurs ne divulgueront ni n'utiliseront aucune information confidentielle à des fins autres que celles liées à l'exercice de leurs responsabilités professionnelles/contractuelles, sauf autorisation expresse d'Airbus.

6.3 Les Utilisateurs devront respecter la classification des informations telle que définie par Airbus dans sa directive « Security Requirements for Company Data Classification and Protection» (A1044) et/ou par les lois et les règlements en vigueur.

7. SECURITE

7.1 Mesures d'authentification et de sécurité

7.1.1 Les Utilisateurs devront sécuriser physiquement tous leurs appareils mobiles tels qu'ordinateurs portables, supports amovibles, téléphones mobiles, tablettes, etc., et garantir leur manipulation adéquate afin d'éviter leur vol ou leur perte. En particulier, ils ne devront jamais laisser ces appareils sans surveillance dans les lieux publics ou les zones des locaux d'Airbus auxquelles les visiteurs peuvent accéder librement.

7.1.2 Les Utilisateurs doivent se déconnecter ou activer un économiseur d'écran protégé par mot de passe lorsqu'ils laissent leur PC et leurs appareils mobiles sans surveillance, y compris pour une courte durée.

7.1.3 Seuls les supports amovibles ayant été approuvés/fournis par le Département IM doivent être connectés aux Moyens IS&T. Sauf dans le cas où le Département IM a fourni un équipement approprié, les supports amovibles (par ex. clés USB et disques durs) devront être utilisés uniquement pour le transfert de données et non pour leur stockage. Toutes les données confidentielles devront être protégées par des moyens appropriés qui seront fournis aux Utilisateurs par le Département IM.

7.1.4 Les Utilisateurs devront assurer la stricte confidentialité de leurs mots de passe et codes d'accès. Aucune trace écrite de ces informations ne doit être conservée ; ces informations ne doivent pas non plus être enregistrées à des fins de connexion automatique (par ex., dans une macro ou une touche de fonction), excepté si ces méthodes sont validées par le Département Sécurité. Si un Utilisateur soupçonne qu'une personne non autorisée a pu obtenir son mot de passe ou ses codes d'accès, il devra immédiatement modifier ces informations et en informer le Département Sécurité d'Airbus.

7.1.5 Les Utilisateurs auxquels ont été fournis des logiciels pour faciliter l'authentification de l'accès à distance devront protéger ces outils contre la perte ou le vol, et protéger leur code PIN de la même manière que leurs mots de passe. Les outils d'authentification et d'accès sécurisés ne doivent jamais être partagés entre plusieurs utilisateurs. Les Utilisateurs devront notifier dans les meilleurs délais la perte ou le vol de leurs outils d'authentification et d'accès sécurisés au Département Sécurité d'Airbus, au Département IM et/ou au responsable d'atelier.

7.2 Stockage et rétention

7.2.1 Toutes les données professionnelles devront être stockées par l'Utilisateur, à des fins de sauvegarde, dans les fichiers/stockages en réseau appropriés des Moyens IS&T.

7.2.2 Si un Utilisateur rencontre des difficultés pour stocker des données professionnelles sur un appareil spécifique ou a des besoins spécifiques et justifiés en termes de stockage, il doit contacter le Département IM.

7.2.3 En cas de suppression accidentelle de données professionnelles, l'Utilisateur doit en informer immédiatement le Département IM local.

7.2.4 Sous réserve des lois et règlements locaux, l'utilisation des Moyens IS&T (communication de données) par tous les Utilisateurs peut être enregistrée par Airbus et conservée pendant un délai d'un an (par ex., historique de navigation sur Internet).

7.2.5 L'Utilisateur peut demander au DPO local le droit d'accéder aux informations concernant le stockage et la rétention.

8. SURVEILLANCE

8.1 Objet et domaine d'application

8.1.1 Airbus pourra surveiller toutes les activités impliquant les Moyens IS&T.

8.1.2 Cette Surveillance pourra entraîner le déploiement de différents outils permettant de protéger les Moyens IS&T. Il peut s'agir par exemple de programmes antivirus, de mécanismes et de logiciels de filtrage pour prévenir la perte de données. Airbus pourra également exploiter un système informatisé pour surveiller les communications sécurisées (telles que le trafic sur le web crypté par SSL).

8.1.3 Cette Surveillance est effectuée aux fins suivantes :

8.1.3.1 Assurer la confidentialité et l'intégrité des infrastructures, des réseaux, des données et des Moyens IS&T d'Airbus ;

8.1.3.2 Assurer une utilisation efficace des Moyens IS&T et leur fonctionnement normal ;

8.1.3.3 Assurer la conformité aux lois et règlements en vigueur et/ou au présent Document ;

8.1.3.4 Enquêter sur toute violation des lois et règlements en vigueur et/ou du présent Document ;

8.1.3.5 Assurer le respect par l'Utilisateur des obligations de sécurité et de confidentialité contenues dans le présent Document ;

8.1.3.6 Identifier, surveiller et protéger les actifs d'Airbus ; et

8.1.3.7 Assurer un contrôle efficace des coûts.

8.2 Exécution de la Surveillance

8.2.1 Les activités de Surveillance devront être menées uniquement par les membres du Département Sécurité d'Airbus, lesquels ont reçu une formation adéquate en termes de protection des données personnelles.

8.2.2 Aux fins énoncées à l'Article 8.1 ci-avant, Airbus pourra surveiller toute utilisation des Moyens IS&T et accéder à toutes les données professionnelles. À cet égard, Airbus pourra surveiller toutes les activités impliquant les Moyens IS&T, y compris les historiques de navigation sur Internet (noms des sites web consultés, durée de navigation, fichiers/matériel téléchargés et bande passante utilisée, etc.), les e-mails envoyés et reçus (y compris les pièces jointes), les fichiers stockés sur les Moyens IS&T (par ex. les fichiers PST), les connexions réseau et tous les journaux d'ordre général relatifs aux Moyens IS&T.

8.2.3 Dans l'éventualité d'une détection d'un incident de sécurité, Airbus pourra analyser les mesures de sécurité appliquées (par exemple en effectuant un examen des journaux concernés ou une investigation des Moyens IS&T) pour identifier les causes profondes de l'incident et

prendre des mesures correctives afin de circonscrire les dommages causés aux Moyens IS&T ou aux intérêts d'Airbus.

8.2.4 Afin de prévenir et de pallier un risque imminent pour la sécurité des Moyens IS&T ou des intérêts d'Airbus, Airbus pourra bloquer ou suspendre temporairement l'utilisation et l'accès aux Moyens IS&T pour un Utilisateur.

8.3 Accès aux données « privées » dans le cadre de la Surveillance

8.3.1 L'utilisation occasionnelle des Moyens IS&T à des fins privées est tolérée pour contacter ses proches et effectuer des tâches quotidiennes, toutefois Airbus pourra surveiller toutes les données privées (dossiers, e-mails, fichiers et répertoires, qu'ils soient identifiés « Privé », « Personnel » ou autre) conformément aux dispositions du présent Document.

8.3.2 Les Utilisateurs sont informés que les logiciels déployés par Airbus pourraient ne pas être en mesure de faire la distinction entre les données privées et professionnelles. Les Utilisateurs reconnaissent donc que les activités de Surveillance s'appliquent de la même manière à toutes les données stockées et transmises via les Moyens IS&T.

8.3.3 Dans le cadre strict des lois et règlements en vigueur et en tenant compte des particularismes juridiques nationaux, les membres du Département Sécurité d'Airbus pourront accéder à des données identifiées comme « Privées » comme précisé dans l'article 2.2.4 en cas de suspicion raisonnable d'utilisation illégale ou lorsqu'un tel accès est nécessaire pour prévenir ou pallier un risque imminent ou tout événement nuisant ou susceptible de nuire à la sécurité des Moyens IS&T d'Airbus ou aux intérêts d'Airbus.

9. VIE PRIVEE ET PROTECTION DES DONNEES

9.1 Toutes les Données personnelles collectées auprès des Utilisateurs devront être traitées de manière à garantir la conformité avec les lois en vigueur en matière de protection des données. Seul un représentant d'Airbus dont l'accès a été autorisé pour des raisons techniques, professionnelles et de gestion pourra accéder aux Données personnelles collectées auprès des Utilisateurs.

9.2 En ce qui concerne les questions relatives aux droits sur les données personnelles (par ex. droit de rectification et droit à l'oubli), les Utilisateurs pourront contacter leur DPO local afin de lui soumettre leur demande.

10. SANCTIONS

10.1 S'il est démontré que le non-respect par un Utilisateur des dispositions du présent Document est personnellement imputable audit Utilisateur, sous réserve des lois et règlements locaux, les sanctions suivantes pourront être prises par Airbus :

10.1.1 Mesures disciplinaires ; et/ou

10.1.2 Responsabilité civile et/ou pénale personnelle.

11. ENTREE EN VIGUEUR

11.1 Le présent Document a été présenté à tous les comités d'entreprise et les autorités d'Airbus concernés conformément aux procédures sociales nationales en vigueur, le cas échéant. En tant que tel, ce Document est entré en vigueur le premier janvier 2019.

11.2 Afin de se conformer aux lois et règlements en vigueur et à toute évolution de la politique d'Airbus, le présent Document pourra être modifié par Airbus aussi souvent que nécessaire, sous réserve du respect des procédures sociales nationales en vigueur.

11.3 La dernière version de ce Document sera publiée sur l'Intranet d'Airbus ou communiquée sur simple demande adressée au Département Sécurité d'Airbus.

ANNEXE 1 GLOSSAIRE

Airbus : Airbus SAS et ses filiales, entreprises affiliées, joint-ventures et entreprises affiliées dans lesquelles une quelconque entité Airbus détient une participation majoritaire, y compris leurs sites et implantations.

Département Sécurité d'Airbus : organisation Airbus, y compris toutes les personnes autorisées agissant au nom d'Airbus, responsable de la fourniture, du respect et de la mise en œuvre des exigences, des lignes directrices et des processus de sécurité visant à assurer la protection des informations et des actifs d'Airbus.

Document : le présent document de référence, y compris ses annexes, qui définit les principes et modalités d'utilisation des Moyens IS&T d'Airbus.

Utilisateur : toute personne susceptible d'utiliser ou d'avoir accès aux Moyens IS&T. Les Utilisateurs peuvent être des employés, des stagiaires, des contractants, des prestataires de services, des clients, des visiteurs d'Airbus, disposant d'un accès aux Moyens IS&T, qu'ils soient membres du personnel Airbus ou non Airbus, permanents ou temporaires. À des fins de clarification, les membres du Département IM et/ou du Département Sécurité d'Airbus, ainsi que tous les profils informatiques (par ex. les administrateurs IM) sont inclus dans cette définition.

Département IM : organisation officielle au sein d'Airbus chargée de fournir les Moyens IS&T aux Utilisateurs.

Moyens IS&T : désigne les Systèmes et Technologies de l'Information fournis par Airbus (ou par un prestataire de services pour le compte d'Airbus) aux Utilisateurs afin de leur permettre d'effectuer leurs tâches professionnelles. Ces Moyens sont notamment : PC, ordinateurs portables, supports amovibles, téléphones, tablettes et logiciels, « conteneurs professionnels » installés sur les Moyens IS&T détenus par Airbus ou l'Utilisateur, ainsi que les services et équipements auxiliaires, nécessaires pour soutenir et faciliter le système d'information d'Airbus (par ex. outils de sécurité, traitement d'images de vidéosurveillance et contrôle d'accès).

BYOD : signifie « Bring Your Own Device » et désigne les appareils que les Utilisateurs sont autorisés à utiliser à des fins privées.

Adresse IP/réseau : adresse numérique par laquelle un emplacement sur Internet est identifié et qui permet d'identifier l'ordinateur de l'utilisateur sur le réseau. Les adresses IP Airbus sur Internet sont fixes. Indépendamment de l'adresse IP de son ordinateur sur le réseau Airbus, tout Utilisateur connecté à Internet à partir d'Airbus reçoit une adresse IP Internet appartenant à Airbus et identifie Airbus comme la source de l'activité réalisée.

Données personnelles : toute information concernant une personne physique identifiée ou identifiable. Est réputée identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identificateur en ligne, ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

Sources Internet non fiables : désigne les sites web dont le certificat de sécurité est douteux, auquel cas, votre navigateur Internet vous avertit que le site web doit être traité comme un site non fiable.

Surveillance/surveiller : on entend par Surveillance l'ensemble des procédés automatisés de filtrage, de trie et de traçage des flux et des données transitant sur les systèmes d'information d'Airbus. Ces procédés, qui impliquent un contrôle automatique et indiscriminé des fichiers et de leur contenu, ne nécessitent pas la visualisation systématique des données par une personne physique.

ANNEXE 2 FAQ

Sujets/Questions	Réponses
Objectifs de la Charte sur les Moyens IS&T	La présente Charte sur les Moyens IS&T a pour objectif de consolider et d'harmoniser les règles d'Airbus relatives à l'utilisation des Moyens IS&T par les Utilisateurs. Le regroupement de ces règles dans un document commun a permis de clarifier les conditions d'utilisation et de renforcer la protection d'Airbus et des Utilisateurs, tout en assurant la fonctionnalité du présent Document de référence au niveau national.
Pourquoi les « e-mails privés occasionnels », les « utilisations privées occasionnelles d'Internet » ou toute « utilisation privée occasionnelle des Moyens IS&T d'Airbus » sont-ils autorisés dans certains pays, mais pas dans d'autres ?	Comme expliqué, le présent Document a été développé afin d'harmoniser les règles liées à l'utilisation des Moyens IS&T par les Utilisateurs. Dans la mesure où les législations nationales relatives à l'utilisation des Moyens IS&T diffèrent d'un pays à l'autre, il n'est pas toujours possible d'adopter une approche globale pour tous les problèmes potentiels. Dans certains pays, la jurisprudence indique que les Moyens IS&T fournis par un employeur peuvent être utilisés à des fins privées, à condition que cette utilisation soit raisonnable et n'empêche pas les employés d'effectuer leur travail. Dans d'autres pays, cela n'est pas autorisé. La direction d'Airbus a donc décidé, dans le respect de la législation nationale, de restreindre autant que possible l'utilisation des Moyens IS&T aux fins privées. **Le principe de base est que** les Moyens IS&T ne doivent pas être utilisés dans le cadre d'activités non professionnelles, excepté s'il s'agit d'une utilisation mineure et exceptionnelle (par ex., en cas d'urgence ou d'interruption en déplacement, ou encore pour contacter ses proches). Les Utilisateurs devront adopter une approche fondée sur le bon sens dans leur utilisation des Moyens IS&T à des fins privées.
Dans le cas où un Utilisateur est basé à l'étranger, mais qu'il a un contrat avec une entité Airbus basée dans son pays d'origine, comment est régie l'utilisation des Moyens IS&T pour raisons privées ?	L'utilisation des Moyens IS&T pour raisons pivées est soumise aux règles du pays d'origine.
Je travaille à l'étranger et souhaite utiliser les Moyens IS&T pour communiquer avec ma famille et lui apporter mon soutien. Est-ce possible ?	Il n'existe pas de droit spécifique permettant l'utilisation des Moyens IS&T par des employés à des fins privées. Cependant, les tribunaux sont souvent disposés à conclure que les employés peuvent faire un usage privé raisonnable des Moyens IS&T mis à disposition par l'employeur, à la condition que cette utilisation n'interfère pas avec leurs tâches professionnelles.

	Les employeurs ne sont pas tenus d'autoriser l'utilisation du matériel de communication par des employés à des fins privées. Cependant, de nombreux employeurs choisissent de le faire. Afin d'assurer l'intégrité et la confidentialité du système, la direction d'Airbus a décidé d'interdire aux employés d'utiliser les Moyens IS&T à des fins privées dans certains pays, à savoir, les pays où une telle interdiction est autorisée.
Les dispositions de la Charte sur les Moyens IS&T s'appliquent-elles lorsque les Moyens IS&T sont utilisés en dehors des heures de travail pour accéder à des sites web non professionnels ?	Les stipulations de la Charte sur les Moyens IS&T sont applicables à tous les Moyens IS&T, qu'ils soient utilisés au bureau, à domicile, dans un hôtel, etc.
Comment savoir quels documents sont confidentiels ?	Le document de référence intitulé **A1044 « Security Requirements for Company Data Classification and Protection»** explique comment établir cette détermination. Le document de référence A1044 est disponible sur le portail/Hub Intranet d'Airbus.
Comment puis-je utiliser les outils de cryptage ?	Si nécessaire, et sous réserve de validation par l'homologue Airbus, des outils de cryptage peuvent être fournis aux Utilisateurs par Airbus. Sous réserve que ces conditions soient remplies, vous pouvez utiliser plusieurs outils de cryptage. Ces outils ont des applications différentes : certains peuvent crypter des dossiers et des e-mails spécifiques, d'autres la totalité du disque dur. Le cryptage peut être effectué : • par vous-même (pour Airbus) : Start/PC Services/All/ « nom de l'outil de cryptage » ; ou • vous pouvez appeler votre ISR ; ou • contactez votre Département IM local. Si vous cryptez la totalité d'un disque dur, il est recommandé de le faire le soir car cette opération peut être longue.
Où dois-je stocker mes archives lorsque mon disque habituel est plein ?	Conformément à l'Article 7.2 ci-avant, toutes les données professionnelles devront être stockées sur le disque dur de l'appareil de réception ou de création des données. Si vous rencontrez des difficultés à stocker vos données

	professionnelles, vous devez contacter le Département IM dans les meilleurs délais.
Airbus surveille-t-il régulièrement l'utilisation d'Internet ?	Airbus surveille l'utilisation d'Internet. Toutefois, Airbus est parfois contraint d'accéder aux activités des utilisateurs sur le web (et consulter leurs données personnelles/privées) afin d'identifier des menaces de sécurité informatique.
Accès BYOD	Airbus considère que les fichiers personnels/privés se trouvant hors du conteneur professionnel sur un appareil BYOD ne sont pas de nature professionnelle. En conséquence, Airbus n'accèdera pas à ces fichiers sans le consentement exprès de l'Utilisateur (ou sur autorisation judiciaire).
Vous avez des questions sur les smartphones ?	Consultez https://smartphone.airbus.corp/faq/