Charte Informatique
Airbus Defence and Space France

OBJECTIF :

La présente Charte définit les règles applicables à l'utilisation des Ressources Informatiques au sein d'Airbus Defence and Space en France.

CADRE :

Airbus Defence and Space France : Airbus Defence and Space SAS, Airbus DS Geo SA, Airbus DS Secure Land Communications SAS, Cassidian Cybersecurity SAS

Propriétaire du document :

Nom : BOURGETEAU, Kévin

Fonction : OSSI Airbus DS Geo SA

Autorisé pour application :

Nom : MOREL, Eric

Fonction : OCSSI France, Airbus Defence and Space SAS

Table des matières

1 Objet et domaine d'application

La présente charte vient compléter la charte « Information Management & Utilisation des Moyens IS&T d'Airbus » pour tenir compte des spécificités liées à l'Utilisation des Ressources Informatiques au sein d'Airbus Defence and Space en France.

La Division Airbus Defence and Space en France étant soumise à des règles d'utilisation des Ressources Informatiques spécifiques et en l'absence de règles spécifiques donnant des indications contraires (exemple : réseau « Divisional », télétravail, données classifiées de Défense, « BYOD » (Bring Your Own Device), procédures d'utilisation de certains équipements de mobilité (smartphones, etc.)), les règles reprises au sein de la présente charte sont applicables à tous les Utilisateurs travaillant avec des Ressources Informatiques d'Airbus Defence and Space.

Elle s'applique au sein des sociétés Airbus Defence and Space SAS, Airbus DS Géo SA, Airbus DS Secure Land Communications SAS et Cassidian Cybersecurity SAS.

2 Confidentialité de l'information

2.1 Les ressources informatiques sont cloisonnées pour tenir compte des divers niveaux de sensibilités. Ainsi, pour des environnements de sensibilités différentes, des réseaux informatiques, physiquement séparés, sont mis à disposition par Airbus Defence and Space. L'Utilisateur ne doit pas connecter de Ressource Informatique délivrée pour un environnement défini sur un autre environnement.

La liste des différents réseaux informatiques listés du plus sensible au moins sensible sont les suivants :

- Les réseaux classifiés de défense qui sont réservés pour le traitement des données classifiées de défense uniquement[1] ;
- Le réseau National réservé au stockage et au traitement des données soumises aux règlementations nationales[2] ;
- Le réseau Divisional pour le stockage et le traitement des données non nationales.

2.2 Toutes informations professionnelles[3] doivent être stockées et sauvegardées sur le Système d'Information d'Airbus Defence and Space en regard de sa sensibilité et du besoin d'en connaitre.

2.3 Dans le cadre de travail collaboratif, il convient de s'assurer que les outils mis à disposition (Webex, Sharepoint, partage d'écran, chat, visioconférence) sont aptes à supporter le niveau de sensibilité des informations échangées.

2.4 L'Utilisateur doit informer sa hiérarchie de toute demande de renseignement sur les Ressources Informatiques d'Airbus Defence and Space ou d'Airbus.

2.5 L'Utilisateur ne doit pas communiquer à des personnes non autorisées à les recevoir des informations professionnelles.

[1] Information ou support protégé dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale. L'accès est restreint aux personnes préalablement habilitées et justifiant du besoin d'en connaître d'après l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 30 novembre 20 Il sur la protection du secret de la défense nationale.

[2] Regroupe les informations sensibles au sens de l'instruction interministérielle relative à la protection des systèmes d'information sensibles n° 901/sgdsn/anssi « Informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre ». Et les informations relevant de la protection du potentiel scientifique et technique de la nation défini par le décret n°2011 -1425 du 2 novembre 2011 et l'arrêté du 3 juillet 2012 tel que « le dispositif de protection du potentiel scientifique et technique de la nation (PPST) a pour but de protéger, au sein des établissements publics et privés, l'accès à leurs savoirs et savoir-faire stratégiques ainsi qu'à leurs technologies sensibles ».

[3] Les informations ou données professionnelles sont toutes données ou informations ayant été apprises, comprises, connues ou devinées à l'occasion de l'exercice professionnel de l'Utilisateur. Ces informations ou données peuvent être de nature technique ou avoir trait aux activités commerciales. Ces informations, matérielles, immatérielles ou orales sont confidentielles qu'elles soient longues ou brèves et que l'Utilisateur juge qu'elles aient une valeur moindre ou inestimable.

3 Courrier électronique

L'article 3 « COURRIER ELECTRONIQUE » de la charte « Information Management & Utilisation des Moyens IS&T d'Airbus » est complété au sein d'Airbus Defence and Space France par les dispositions suivantes :

3.1 L'Utilisateur doit :

3.1.1 Effectuer tout envoi, interne ou externe, d'informations nécessitant l'intégrité des données envoyées en signant ses mails avec les outils mis à disposition par Airbus Defence and Space ;

3.1.2 Effectuer tout envoi, interne ou externe, d'informations sensibles en utilisant les moyens de chiffrement en vigueur au sein d'Airbus Defence and Space, qualifiés pour le niveau de sensibilité des informations ;

3.1.3 Effectuer tout envoi, interne ou externe, d'informations soumises aux règlementations nationales à partir de sa messagerie nationale Airbus Defence and Space.

3.2 De plus l'Utilisateur ne doit pas :

3.2.1 Synchroniser des équipements personnels (téléphones portables, tablettes, Smartphone, etc.) avec un compte de messagerie professionnel ;

3.2.2 Émettre ou transmettre des e-mails et pièces jointes d'ordre professionnels contenant ou non des informations sensibles à un compte de messagerie personnel ;

3.2.3 Communiquer des e-mails et des informations non conformes aux règles Airbus Defence and Space et/ou aux lois et réglementations applicables.

4 Internet et Intranet

L'article 4 « INTERNET/INTRANET » de la charte « Information Management & Utilisation des Moyens IS&T d'Airbus » est complété au sein d'Airbus Defence and Space France par les dispositions suivantes :

4.1 Toute activité exercée par l'Utilisateur sur Internet ou sur l'Intranet peut porter atteinte à l'image d'Airbus Defence and Space et/ou engager sa responsabilité. En effet tous les Utilisateurs connectés à Internet depuis Airbus Defence and Space reçoivent une adresse IP Internet qui appartient à Airbus Defence and Space et permet d'identifier Airbus Defence and Space comme étant la source de l'activité. L'adresse IP/Réseau est l'adresse numérique par laquelle une localisation sur Internet est identifiée, et qui permet d'identifier l'ordinateur de l'Utilisateur sur le réseau.

4.2 De plus l'accès à Internet depuis l'environnement privé des téléphones mobiles professionnels s'effectue sans contrôle et engage donc la responsabilité pleine et entière de l'Utilisateur.

4.3 Afin d'assurer la protection des données sensibles échangées, et notamment pour se protéger des sources d'exfiltration de donnée, l'Utilisateur doit donc utiliser les sites d'échange et de diffusion de données, de contenu et de fichiers en stricte conformité aux contextes d'emploi validés par Airbus Defence and Space, notamment au regard de la sensibilité des informations concernées, de la localisation des sites externes, et des moyens d'accès.

4.4 Il est impératif de sécuriser les échanges de données sensibles au travers d'Internet en utilisant des moyens de chiffrement qualifiés pour le niveau de sensibilité des données échangées, (par exemple Stormshield Data Security (Security Box), ou des chiffreurs qualifiés par l'ANSSI). Ainsi seuls les destinataires doivent pouvoir accéder à ces informations partagées.

4.5 Il convient également d'adopter un comportement responsable et d'appliquer son devoir de discrétion par rapport aux activités professionnelles, dès lors que des informations de l'entreprise sont publiées et/ou échangées sur Internet, même à l'extérieur de la société ou en dehors des heures de travail, pour communiquer des informations confidentielles sur Airbus Defence and Space (exemple : diffusion d'informations sur des sites web, des chats, des forums, des blogs, des réseaux sociaux ou sur tout autre support).

4.6 De plus l'Utilisateur ne doit pas :

4.6.1 Utiliser, hors règles spécifiques (par exemple accord sur le télétravail), des services de télécommunication (« box » par exemple) autre que ceux proposés par le Service Informatique ;

4.6.2 Télécharger, enregistrer, installer, désinstaller, actualiser, utiliser ou distribuer des fichiers, des programmes, des codes ou des logiciels d'Internet, sans l'autorisation du Service informatique ou de l'équipe Sécurité d'Airbus Defence and Space même à titre provisoire ou pour un essai ou même si ce sont des programmes à licence libre ;

4.6.3 Créer des sites web indépendants sur Internet. Toutes les informations d'Airbus Defence and Space seront publiées sur les sites officiels Airbus Defence and Space.

5 Mobilité et medias amovibles

L'article 5 « MOYENS IS&T MOBILES» de la charte « Information Management & Utilisation des Moyens IS&T d'Airbus » est complété au sein d'Airbus Defence and Space France par les dispositions suivantes :

5.1 La sécurité de la mobilité et des médias amovibles constituent l'un des principaux enjeux sécuritaires auxquels Airbus Defence and Space doit s'adapter pour préserver son patrimoine informationnel. Les équipements de mobilité : téléphones connectés (ordi phones/smartphones), ordinateurs portables, tablettes et médias amovibles (clé USB, cartes mémoires, etc.), favorisent le transport et la diffusion de données d'Airbus Defence and Space hors de ses sites, mais les exposent aussi plus facilement aux risques et aux menaces (comme la perte et le vol).

5.2 Les régimes de télétravail et d'astreinte étant des cas particuliers de mobilité, ils nécessitent des règles complémentaires et la mise en place de modalités clairement définies par les Ressources Humaines.

5.3 En cas de déplacement dans un environnement non maîtrisé il faut :

5.3.1 Rester vigilant, lors de l'utilisation des équipements de mobilité (exemple : utilisation des téléphones portables ou de l'ordinateur portable dans des lieux publics) ;

5.3.2 Demander au Service Informatique un PC blanc pour tout déplacement professionnel en dehors de l'Union Européenne et y mettre uniquement les données strictement nécessaires à la mission ;

5.3.3 Stocker en local sur son équipement de mobilité que les données nécessaires à sa mission, surtout si celles si sont des données sensibles.

5.4 En cas d'utilisation de connexion hors réseau filaire d'Airbus Defence and Space, il faut :

5.4.1 Être, en toute circonstance, extrêmement prudent sur les informations transmises par téléphone portable, ces systèmes n'offrant aucune sécurité (écoute des systèmes de communication) ;

5.4.2 Utiliser les accès au réseau Internet proposés par certains équipements mobiles en passant par l'infrastructure sécurisée d'Airbus Defence and Space. C'est notamment le cas pour les accès "DATA" des téléphones portables. Ce type d'accès ne doit pas être utilisé à des fins professionnelles. Toute utilisation à des fins professionnelles doit être réalisée au travers de l'infrastructure d'Airbus Defence and Space, c'est-à-dire une fois la connexion VPN établie.

5.5 Il convient également de :

5.5.1 Protéger ses outils d'authentification et d'accès sécurisé pour l'authentification de l'accès à distance, contre toute perte, ou vol ou utilisation par un tiers, et protéger leur code de la même manière que ses mots de passe. Comme les mots de passe, les outils d'authentification et d'accès sécurisés ne doivent jamais être partagés avec d'autres Utilisateurs ;

5.5.2 Ne pas activer et/ou utiliser sur ses équipements bureautiques le réseau sans fil (exemple : Bluetooth, WIFI..) à proximité et dans les zones sécurisées de défense ;

5.5.3 Ne pas utiliser son téléphone portable dans les zones signalées par un pictogramme.

6 Sécurité de l'environnement de travail

6.1 Les informations d'authentifications (identifiants, mots de passe, etc.) sont des données sensibles, incessibles et confidentielles, l'Utilisateur doit donc les manipuler comme tel et notamment :

6.1.1 S'assurer que le stockage électronique et/ou la diffusion à un tiers d'un mot de passe (ex. compte VPN d'un client, mot de passe d'un document chiffré, etc.) sont en conformité avec les règles d'Airbus Defence and Space en matière de protection et de chiffrement des informations d'authentification ;

6.1.2 Modifier, à la première connexion, les informations initiales d'authentification qui sont fournies par le Service Informatique. Il est de la responsabilité de chaque Utilisateur de choisir un mot de passe qui soit conforme aux politiques de sécurité d'Airbus Defence and Space.

6.2 Afin de préserver le patrimoine informationnel de l'entreprise et pour assurer la continuité de l'activité il est impératif de stocker toutes les données professionnelles, à des fins de sauvegarde, sur des ressources (serveur du réseau) d'Airbus Defence and Space. Le Service Informatique effectue des sauvegardes régulières de ses Systèmes d'Information. Si malgré tout, des données sensibles doivent être stockées en local sur un moyen informatique, elles doivent être chiffrées avec un outil de chiffrement qualifié.

6.3 Tout nouveau besoin de création d'un Système d'Information doit être discuté avec le BRM (Business Relationship Manager) correspondant. Le Service Informatique devra être informé de ce besoin business afin notamment de procéder aux mesures d'enregistrement de ce nouveau Système d'Information.

6.4 Afin qu'Airbus Defence and Space maitrise ses Ressources Informatiques, les Utilisateurs ne doivent pas :

6.4.1 Établir une connexion simultanée à un réseau secondaire sur un poste connecté au réseau local. Par exemple, il ne faut jamais utiliser un modem, un partage de connexion avec un Smartphone, un réseau sans fil, une carte 3G, etc. quand le poste de travail est connecté au réseau local ;

6.4.2 Utiliser des moyens d'échanges de données qui ne sont pas exclusivement autorisés et/ou gérés par le Service Informatique. Que ce soit pour des échanges externes (ex. Google docs, etc.) ou des échanges internes (ex. partages réseaux, etc.) ;

6.4.3 Introduire ou installer des dispositifs électroniques non autorisés tels que des routeurs sans fil, câble, etc. susceptibles de nuire au fonctionnement du réseau et de générer des risques d'accès non autorisés ;

6.4.4 Ajouter ou retirer des éléments matériels de son poste de travail (RAM, disque dur interne, batterie, etc.).

7 Statut de la charte et Sanction

La présente charte constitue une adjonction au règlement intérieur, au sens de l'article L. 1321-5 du Code du Travail.

En conséquence, les sanctions disciplinaires applicables en cas de non-respect de la présente Charte, sont énoncées au sein du Règlement Intérieur auquel elle est annexée.

Ainsi :	L'*Utilisateur* peut engager sa responsabilité civile et/ou pénale en cas de non-respect des règles et obligations exposées dans cette Charte, s'il est démontré que ce non-respect est directement imputable à l'Utilisateur en cause
	Airbus Defence and Space est en mesure de se retourner contre l'*Utilisateur* qui aurait fait une mauvaise utilisation avérée d'Internet ou des Ressources Informatiques en ne respectant pas les règles établies par le présent document

Toute modification ultérieure, adjonction ou retrait à la présente charte, fera l'objet de la procédure prévue à l'article L. 1321-4 du Code du Travail.

8 Historique des révisions

Version	*Date*	*Motif de la révision*
1.0	19/01/2018	Création du document
1.1	20/02/2018	Révision après information des CE
1.2	31/07/2018	Révision en parallèle de la mise en place de la charte « Information Management & Utilisation des Moyens IS&T d'Airbus »