REFERENCE	INDICE	DATE
DGSI 036846	**F**	**23/05/2025**

Charte de bon usage du système d'information

DG

DOMAINE

Sécurité des Systèmes d'Information

Approuvé

Direction Générale du Système d'Information

Edition	*Date*	*Indice*		*Visa Rédacteur*	*Visa Approbateur*
Origine	16/05/2012		JP. Weber	Christophe Floch - 00033689 2025.05.23 09:48:33 +02'00'	Laurent Bendavid - 00068536 Signature numérique de Laurent Bendavid - 00068536 Date : 2025.05.25 10:53:15 +02'00'
Dernière mise à jour	23/05/2025	F	C. Floch	C. Floch	L. Bendavid

TABLE DES MATIERES

1. PRÉAMBULE ET CHAMP D'APPLICATION

La présente charte a pour objet de définir les règles d'utilisation des outils numériques au sein de DASSAULT AVIATION (ci-après « la Société »). Elle s'applique à toute personne physique (ci-après « l'Utilisateur »[1]) disposant d'un accès aux services et équipements numériques de la Société.

Elle vise à assurer la conformité aux obligations légales et réglementaires, à garantir la sécurité des systèmes d'information (SI) et à favoriser un usage approprié des ressources numériques.

Tout manquement aux dispositions de cette charte est susceptible d'entraîner des sanctions disciplinaires, une suspension conservatoire des outils mis à disposition, une restriction de ses droits d'accès, sans préjudice d'éventuelles actions pénales ou civiles à son encontre. Si l'Utilisateur est un personnel d'une autre entité en contrat avec la Société, d'éventuelles actions pourront être entreprises contre son employeur.

2. CADRE JURIDIQUE ET PRINCIPES GÉNÉRAUX

La Société s'engage notamment à respecter les dispositions législatives et réglementaires suivantes :

DG

- La protection des données personnelles au titre de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que du règlement européen relatif « à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » [UE 2016/679]. Pour plus d'informations, voir la note DEC 23/2024 ;
- Le respect de la vie privée tel qu'indiqué par l'article 9 du code civil ;
- Le secret des correspondances émises par la voie des communications électroniques, tel qu'indiqué dans l'article 226-15 du code pénal ;
- Le Règlement (UE) 2021/016 du 13 juin 2024 du Parlement européen et du Conseil établissant les règles harmonisées concernant l'intelligence artificielle (IA Act) ;
- La législation sur la propriété intellectuelle (code de la propriété intellectuelle) ;
- La lutte contre le téléchargement illégal au titre de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (dite loi HADOPI) ;
- Les règles de protection des systèmes d'information sensibles (Instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles) et de protections des informations relevant du secret de la défense nationale (Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale) ;

[1] Le terme Utilisateur désigne toute personne physique quel que soit son statut (salarié, stagiaire, apprenti, personnel intérimaire, personnel extérieur, sous-traitant, coopérant …) et quel que soit son lieu d'exercice ou son mode de travail (sur site, en télétravail, accès à distance …).

- La règlementation Part-IS (UE) 2022/1645 du 14 juillet 2022 et (UE) 2022/203 du 27 octobre 2022 visant à identifier et à gérer les risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne (safety).
- Le droit à la déconnexion (loi du 8 août 2016).

3. UTILISATION DES OUTILS NUMÉRIQUES

3.1 Utilisation responsable

Les Utilisateurs sont tenus de respecter les principes fondamentaux de réserve, de probité, de neutralité, de respect du secret professionnel et de discrétion. Ils doivent notamment :

- Ne pas tenir des propos contraires à l'ordre public, diffamatoires, racistes, xénophobes, homophobes, portant atteinte à la décence, constituant une diffusion de fausse nouvelle, incitant à la violence ou la haine, portant atteinte aux droits d'autrui (droit à l'image, vie privée, propriété intellectuelle etc.), ou tout propos illégal ;
- Ne pas faire un usage des outils numériques qui soit contraire aux lois et règlementations en vigueur et à la charte d'éthique de la Société ;

Les Utilisateurs doivent faire un usage sobre et responsable des ressources informatiques mises à leur disposition :

DG

- Ils utilisent les outils numériques de manière raisonnée pour limiter la consommation inutile de ressources ;
- Ils restreignent les impressions papier à ce qui est nécessaire ;
- Ils éteignent les écrans en cas d'absence prolongée.

3.2 Postes de travail et terminaux mobiles

La Société fournit aux Utilisateurs le matériel nécessaire à l'exercice de leurs fonctions (ordinateur fixe ou portable, éventuellement : smartphone, clés USB…). Les Utilisateurs s'engagent à :

- Ne pas modifier les paramètres techniques et les politiques de sécurité et à ne pas empêcher les mises à jour des matériels et/ou logiciels qui leur sont fournis ;
- Ne pas installer de logiciels non autorisés par le service informatique ;
- Ne pas retarder au-delà d'une journée la mise à jour des systèmes d'exploitation et des logiciels, notamment ceux liés à la sécurité, sur leur poste de travail ;
- Ne pas détourner de leur usage les ressources informatiques qui leur sont allouées ;
- Déconnecter ou verrouiller leur session lorsqu'ils s'absentent, même temporairement ;
- Déclarer sans délai tout vol ou perte d'un matériel aux services de police, à l'assistance informatique et aux services de sécurité de la Société ;

- Stocker leurs données sur des supports sauvegardés : serveurs bureautiques, solution de gestion électronique des documents (GED) ;
- Limiter le stockage de fichiers personnels en volume et en durée de conservation. Les répertoires partagés et les espaces collaboratifs (SharePoint, Confluence, etc.) ne doivent pas être utilisés à cette fin. Les fichiers personnels sont considérés comme des données professionnelles, sauf mention explicite;
- Ne pas utiliser de matériel personnel à des fins professionnelles, sauf pour accéder aux services numériques mis à disposition à cette fin par la Société (ex : consultation de la messagerie professionnelle sécurisée Citadel Team) ;
- Ne pas connecter au réseau de la Société ou utiliser des équipements qui ne sont pas fournis ou n'ayant pas fait l'objet d'un contrôle par la Société (clefs USB,etc.).

Cas particulier des ordinateurs portables

Ces matériels sont destinés à un usage professionnel.

Ils ne doivent pas être prêtés à des tiers.

En déplacement en dehors des locaux de la Société :

- Les Utilisateurs ne doivent pas laisser leur poste de travail sans surveillance dans un endroit non sécurisé, en particulier dans des lieux publics ;
- Durant les transports la clef d'authentification doit être conservée à un emplacement différent de l'ordinateur portable ;
- Les accès aux réseaux en dehors de nos établissements ne sont autorisés que via des logiciels fournis par la Société, par exemple par l'emploi d'un VPN (virtual private network). L'accès à des ressources sur internet en direct est interdit.

DG

3.3 Usage professionnel et usage privé

Sauf consigne ou autorisation explicite, les outils numériques fournis par la Société sont destinés à un usage professionnel. Un usage personnel modéré peut être toléré, à condition qu'il soit licite, raisonnable et qu'il ne compromette ni la sécurité, ni le bon fonctionnement des services.

Par défaut, les données produites sont réputées professionnelles, sauf mention explicite indiquant un caractère personnel. Seuls les espaces, répertoires, fichiers et/ou messages qualifiés expressément de « personnels » ou de « privés » seront considérés comme tels.

Dans tous les cas, y compris pour un usage privé, l'utilisation doit être conforme à l'ordre public et aux bonnes mœurs et ne doit pas nuire à l'intégrité, à la réputation ou à l'image de la Société

Un usage inapproprié au regard de la présente charte, pourra être regardé comme une faute professionnelle et entrainer les conséquences listées en préambule.

3.4 Messagerie électronique

L'utilisation de la messagerie électronique professionnelle implique, pour les Utilisateurs, le respect des engagements suivants ;

- Faire un usage raisonné de la messagerie et éviter de surcharger les boîtes de messagerie internes ou externes ;
- Ne pas diffuser de messages de type canulars (hoax), chaînes, escroquerie par hameçonnage (phishing), jeux ou paris ;
- Ne pas utiliser leurs adresses professionnelles pour des usages non liés à l'activité de la Société, notamment pour des inscriptions sur des sites commerciaux, forums ou réseaux sociaux ;
- Ne pas rediriger les messages professionnels qu'ils reçoivent sur leur messagerie professionnelle vers une messagerie personnelle ;
- Ne pas utiliser leurs adresses de messageries personnelles dans un contexte professionnel ;
- S'assurer, à chaque envoi de données, en particulier sensibles, que la liste de diffusion ne comporte pas de destinataire inapproprié ;

DG

- Ne pas ouvrir les messages douteux et les pièces jointes suspectes, ne pas répondre aux émetteurs, et ne pas cliquer sur les liens présents dans ces messages ;
- Prévenir le service de traitement des incidents de sécurité informatique en cas de doute ou après avoir ouvert un message ou cliqué sur un lien qui s'avère a posteriori douteux ;
- Faire un usage raisonnable et limité de la messagerie professionnelle pour des finalités personnelles (sauf mention explicite dans l'objet des messages, ils sont considérés comme des données professionnelles) ;
- Supprimer tous les messages et/ou pièces jointes contenant des données à caractère personnel dont la conservation n'est pas justifiée au regard du RGPD.

Tout message électronique envoyé depuis la messagerie professionnelle engage non seulement la responsabilité et l'image de l'Utilisateur mais aussi celle de la Société.

3.5 Carnet d'adresses, agenda et espaces collaboratifs

Les carnets d'adresses, agendas partagés et outils collaboratifs fournis par la Société doivent être utilisés dans un cadre exclusivement professionnel, sauf mention explicite contraire. Toute information saisie dans ces espaces est réputée professionnelle.

Les Utilisateurs s'engagent à :

- Supprimer leurs contacts professionnels lorsqu'ils ne sont plus nécessaires à leurs activités ;
- Ne pas partager les coordonnées d'un tiers sans son consentement préalable ;
- Effacer les données d'un correspondant qui en fait la demande ;
- Gérer avec précaution la visibilité de leurs agendas, de leurs disponibilités, ou de toute donnée publiée sur les espaces collaboratifs mis à disposition ;
- Prendre toutes les mesures nécessaires pour protéger les données personnelles éventuellement partagées via ces outils.

3.6 Identifiants et mots de passe

Les outils numériques fournis par la Société requièrent une authentification. Les moyens d'authentification fournis par la Société, quels qu'ils soient, sont strictement personnels et confidentiels.

Les Utilisateurs s'engagent à :

- Ne pas communiquer à autrui leurs identifiants, mots de passe et/ou clés d'authentification, sauf en cas d'obligation légale ;
- Utiliser des mots de passe suffisamment robustes et différents suivant les usages et les environnements ;

DG

- Changer régulièrement les mots de passe suivant les consignes de sécurité applicables ;
- Réserver les moyens d'authentification professionnels à des usages strictement professionnels ;
- Différencier les mots de passe à usage professionnel de ceux à usage privé ;
- Réserver la signature de documents par un certificat numérique fourni par la Société à un usage professionnel ;
- Signaler immédiatement la perte, le vol ou la compromission d'un moyen d'authentification (token d'authentification).

Les services informatiques mettent à la disposition des Utilisateurs un « coffre-fort logiciel » de gestion des mots de passe pour aider à leur mémorisation.

3.7 Accès à internet

L'accès des Utilisateurs à internet est conditionné au suivi d'une formation initiale à la sécurité numérique. Afin d'assurer le respect des obligations qui lui incombent, la Société met en place les mesures suivantes :

- Un dispositif de sécurisation de la navigation internet via une infrastructure de déport et d'isolation des navigateurs ;

- Des dispositifs de filtrage des accès, limitant l'accès aux seules catégories de sites autorisées ;
- Des mécanismes de collecte des informations d'accès des Utilisateurs à internet.

De manière générale, les Utilisateurs sont invités à faire preuve de sens critique vis-à-vis des contenus disponibles sur internet.

Il est rappelé que certains sites internet sont régis par le droit d'autres États n'offrant pas de garanties de protection des données personnelles. Les Utilisateurs sont incités à prendre toutes les précautions utiles lorsqu'ils les consultent.

3.8 Intelligence artificielle

L'usage d'outils ou de services intégrant des technologies d'intelligence artificielle (IA) par les Utilisateurs est strictement encadré afin de garantir la protection des données, le respect des réglementations en vigueur et la maîtrise des risques pour les activités de la Société.

Tout recours à des solutions d'IA, qu'elles soient internes ou accessibles en ligne (IA génératives, assistants virtuels, analyse automatique, etc.), doit répondre aux principes suivants :

- Être conforme à la politique interne d'utilisation de l'intelligence artificielle au sein de la Société (DEC 5/2025[2]) ;
- Ne pas conduire à une fuite d'informations sensibles, confidentielles ou soumises au secret professionnel ;
- Ne pas traiter de données personnelles sans respect des exigences du RGPD ;
- Ne pas servir à contourner des processus de validation, de conformité ou de contrôle interne ;
- Ne pas produire ou relayer des contenus générés de manière automatisée sans vérification humaine et sans traçabilité.

DG

L'Utilisateur est personnellement responsable des informations transmises à ces outils, ainsi que des résultats ou contenus qu'il pourrait exploiter. Des contrôles peuvent être mis en place pour assurer le respect de ces exigences.

3.9 Téléphonie

La téléphonie fixe professionnelle est mise à disposition des Utilisateurs pour l'exercice de leur activité professionnelle. La Société peut limiter l'accès à certaines fonctions qui ne sont pas nécessaires aux activités professionnelles de l'Utilisateur, telles que les appels internationaux et les numéros surtaxés.

[2] Accessible sur le portail de la Direction de l'Éthique et de la Conformité (DEC)

4. SÉCURITÉ ET CONFIDENTIALITÉ DES INFORMATIONS

4.1 Comportements attendus des Utilisateurs

Les Utilisateurs s'engagent à :

- Respecter les principes de confidentialité, du respect du secret et de discrétion professionnelle ;
- Ne pas communiquer d'informations confidentielles à des personnes non autorisées ou n'ayant pas besoin d'en connaître ;
- Protéger les données avec les moyens adaptés et prescrits par les services de sécurité de la Société ;
- Signaler sans délai au service d'assistance informatique ou au service de sécurité des systèmes d'information de la Société tout vol ou perte de matériel, et tout événement inattendu ou anomalie concernant les systèmes numériques, notamment ceux susceptibles d'avoir une incidence sur la sécurité aérienne ;
- Participer aux actions de sensibilisation à la sécurité de l'information organisées par la Société ;
- Prendre connaissance des communications générales de sécurité et suivre les consignes et fiches techniques de sécurité publiées dans le Portail Cybersécurité[3].

DG

4.2 Données sensibles et données personnelles

Le traitement des données sensibles, dont la divulgation, la perte ou l'altération pourrait porter préjudice à la Société, au secret de défense nationale ou au potentiel scientifique et technique de la Nation, fait l'objet de dispositions particulières.

En particulier, les utilisateurs s'engagent à :

- Marquer les éléments (documents, messages etc.) contenant des informations sensibles ;
- Porter une attention particulière à la protection et à la diffusion de ces informations ;
- Utiliser les moyens de chiffrement mis à leur disposition lorsqu'ils les transfèrent par Internet (messagerie électronique, service de transfert de fichier, outils collaboratifs etc.)

Les Utilisateurs doivent traiter des données personnelles en conformité avec les dispositions de l'Instruction RGPD de la Société (DEC-22022[4]). Ils s'engagent notamment à :

- Respecter les droits des personnes concernées, les finalités et les durées de conservation des données à caractère personnelle conformément aux dispositions de l'Instruction RGPD ;

[3] Accessible à l'adresse https://np.dassault-avion.fr/grp/informatique/porcyber
[4] Accessible sur le portail RH pour les salariés Dassault Aviation, sur le portail de la Direction de l'Éthique et de la Conformité (DEC) et à l'adresse https://info.dassault-aviation.pro/si-legal/

- Faire appel, en cas de doute, au Correspondant à la Protection des Données (CPD) de leur Direction ou au Délégué à la Protection des Données personnelles (DPD).

4.3 Droits d'accès des Utilisateurs

Les Utilisateurs accèdent aux ressources informatiques (réseaux, applications, serveurs, etc.) dans la limite des droits d'accès qui leur sont accordés par des mécanismes d'habilitation.

En application du principe du "moindre privilège", l'Utilisateur ne doit disposer que des privilèges nécessaires à l'accomplissement de ses missions sur les ressources informatiques.

Les privilèges permettant l'administration technique de ces ressources doivent être strictement réservés aux équipes en charge de l'exploitation et du support, et utilisés uniquement pour les actions d'administration le nécessitant.

Toute dérogation à ces règles doit faire l'objet d'une justification formelle par le responsable hiérarchique de l'Utilisateur et d'une validation par les services informatiques. L'Utilisateur doit être sensibilisé aux responsabilités et aux risques de compromission des ressources informatiques associés à l'utilisation de ces privilèges spécifiques.

4.4 Contrôle du respect de la présente charte

DG

La Société met en œuvre des dispositifs de contrôle et de supervision, notamment afin de :

- Veiller au respect de la présente charte ;
- Protéger les systèmes d'information et les données de la Société contre les actes illicites ou malveillants ;
- Veiller à ce que les usages privés des outils numériques restent raisonnables ;
- Établir des statistiques permettant d'évaluer l'usage qui est fait de certains services et d'en améliorer la qualité ;
- Résoudre des problèmes de fonctionnement ;
- Répondre aux exigences légales.

Ces moyens peuvent prendre la forme de :

- Dispositifs de gestion des droits d'accès et des habilitations des utilisateurs des systèmes d'information et de communication ;
- Contrôles automatisés visant notamment la détection de virus ou de logiciels malveillants, la prévention contre l'usurpation d'identité, la lutte contre les messages non sollicités, la prévention contre les fuites d'informations. Les blocages résultant de ces contrôles sont explicités dans la mesure du possible par des messages d'information à l'Utilisateur ;

- Surveillance, par le biais d'interceptions, des canaux de communication chiffrés, dans des cas spécifiques ;
- Dispositifs de collecte de données et de traces notamment pour :
  - ♦ Les services de messagerie (messagerie électronique, messagerie instantanée) ;
  - ♦ Les passerelles entre les systèmes d'information de la Société et l'extérieur (internet, systèmes d'information des partenaires) ;
  - ♦ L'usage de la téléphonie ;
  - ♦ L'usage des moyens d'impression et de reprographie ;
  - ♦ Les accès aux fichiers ;
  - ♦ Les actions réalisées par les Utilisateurs dans certaines applications ou services collaboratifs ;
  - ♦ L'authentification et l'accès aux moyens informatiques.

Ces dispositifs de contrôle et d'analyse sont élaborés et mis en œuvre en conformité avec la règlementation applicable pour la protection des données personnelles. La Société peut ainsi traiter les données de connexion et de trace évoquées plus haut afin de répondre à l'intérêt légitime de la Société de détection et d'analyse d'éventuels incidents de sécurité

En conséquence, les Utilisateurs peuvent exercer, sur demande auprès du Correspondant RGPD de leur Direction ou au Délégué à la Protection des Données personnelles (via l'adresse mail : rgpd@dassault-aviation.com), leur droit d'accès aux traces des connexions les concernant, pendant leur durée de conservation fixée par la Société à un an, compte tenu de la nature de ses activités. Les Utilisateurs disposent aussi de la possibilité d'introduire une réclamation auprès de l'autorité compétente : la Commission Nationale de l'Informatique et des Libertés (CNIL).

DG

En cas de détection ou de présomption d'anomalies, d'incidents de sécurité ou d'utilisation non conforme des outils numériques mis à disposition, des actions de contrôle peuvent être exercées manuellement par les administrateurs et exploitants des ressources informatiques, notamment en vue de l'identification d'un fait fautif et de son auteur.

Ces données, même si elles relèvent de la tolérance d'usage privé, peuvent être communiquées aux autorités habilitées par la loi disposant d'un droit de communication sur ces données, notamment à l'autorité judiciaire compétente.

5. SITUATIONS PARTICULIÈRES

5.1 Personnel informatique

Le personnel informatique disposant de droits d'accès élevés ou privilégiés aux systèmes d'information (administrateurs, exploitants, personnels de support, etc.) est soumis à des

exigences spécifiques, en complément des obligations générales applicables à tout Utilisateur.

Ces personnels s'engagent notamment à :

- Utiliser leurs privilèges uniquement dans le cadre de leurs missions, pour des finalités légitimes, documentées et conformément aux procédures internes ;
- N'accéder qu'aux données strictement nécessaires à la réalisation de leurs tâches et s'interdire de les divulguer ;
- S'interdire toute manipulation, lecture ou modification non justifiée de données personnelles ou confidentielles ;
- Ne pas utiliser leurs privilèges pour contourner les mécanismes de sécurité ou pour accéder à des services ou ressources à des fins personnelles ;
- Appliquer les consignes et bonnes pratiques en matière de traçabilité, journalisation et alertes de sécurité ;
- Informer leur hiérarchie de tout comportement anormal, usage abusif ou incident relatif à la sécurité des systèmes.

L'exercice d'un accès privilégié implique une sensibilisation renforcée aux enjeux de sécurité et peut donner lieu à des contrôles spécifiques par les équipes responsables de la sécurité des systèmes d'information.

DG

Seuls les personnels habilités au sein de l'équipe de sécurité des systèmes d'information sont autorisés, dans le cadre de leurs missions et sous l'autorité de leur hiérarchie, à déployer ou exploiter des outils d'analyse, de surveillance et de contrôle de la sécurité des systèmes d'information. Ces outils sont utilisés dans le respect des dispositions légales en vigueur, notamment celles relatives à la protection des données personnelles.

5.2 Télétravail

Le télétravail est régi dans la Société par un accord cadre. Les Utilisateurs bénéficient des mêmes droits et sont soumis aux mêmes obligations que les Utilisateurs travaillant sur site, tels que décrits dans la présente charte. Ils s'engagent de plus à :

- Ne travailler que dans les lieux conformes à l'accord cadre ;
- Ne pas utiliser d'autres matériels informatiques que ceux fournis par la Société, à l'exception d'équipements personnels de confort (écran, clavier, souris) qui peuvent être connectés à l'ordinateur portable fourni par la Société ;

Le télétravail se pratiquant en dehors des locaux sécurisés de la Société, les Utilisateurs veillent à :

- Ne pas laisser les informations professionnelles à la vue d'autrui (famille, proche, personnes extérieures susceptibles d'accéder au lieu de télétravail …) ;
- Utiliser un filtre de confidentialité, fourni sur demande par la Société ;

- Déconnecter ou verrouiller leur session lorsqu'ils s'absentent, même pour une courte durée ;
- Arrêter leur PC et à conserver le moyen d'authentification dans un lieu sûr, dans le cas d'une absence plus longue ;
- Protéger le PC contre le vol.

5.3 Déplacements à l'étranger ou chez des tiers

Lors des déplacements à l'étranger ou chez des tiers, une vigilance particulière s'impose. Les Utilisateurs doivent notamment respecter les règles suivantes :

- Éviter d'emporter et de stocker des données sensibles sur les équipements, et privilégier l'accès aux données sensibles via des connexions sécurisées ;
- Effectuer la procédure d'effacement des données locales avant de passer la frontière, en cas de voyage en dehors de l'Union Européenne ;
- Ne pas utiliser du matériel qui n'a pas été fourni par la Société (clef USB, ordinateur public, etc.) ;
- Ne pas se séparer de son matériel ;
- Utiliser un filtre de confidentialité.

DG

5.4 Cas particulier des Utilisateurs extérieurs accédant aux services de la Société depuis des moyens informatiques non fournis par la Société

Dans le cadre de certains contrats, la Société autorise des Utilisateurs d'entités tiers à accéder à des services de la Société depuis des moyens informatiques non fournis par la Société.

Ces Utilisateurs bénéficient des mêmes droits et sont soumis aux mêmes obligations que les autres Utilisateurs, tels que décrits dans la présente charte.

Les règles régissant les moyens d'accès aux services de la Société dépendent du type de liaison informatique utilisée et de la sensibilité des informations accédées. Ces règles sont précisées dans un plan d'assurance sécurité lors de l'établissement du contrat entre la Société et l'entité contractante. Ces règles et la présente charte doivent être communiquées et acceptées par l'Utilisateur avant la fourniture des moyens et des informations de connexion.

L'utilisateur est attentif aux règles sur les identifiants et mots de passe (voir §**Erreur ! Source du renvoi introuvable.**). Les moyens d'authentification (identifiant/mot de passe, certificat/code pin, adresse de messagerie ou autres) fournis par la Société sont strictement personnels, confidentiels et incessibles. En cas d'infraction constatée, les identifiants seront immédiatement désactivés.

5.5 Réseaux sociaux « grand public »

Les réseaux sociaux « grand public » permettent des échanges d'intérêt général ou ciblés, purement privés ou ayant des liens potentiels avec l'activité professionnelle de l'Utilisateur. Accessibles depuis les équipements personnels de l'Utilisateur, ils sont hébergés chez des tiers, et bénéficient d'une audience large, souvent mondiale.

Les Utilisateurs peuvent utiliser ces réseaux sociaux en restant soumis aux mêmes droits et obligations que dans le « monde réel ». Ils sont responsables des contenus (images, vidéos, textes, etc.) et commentaires qu'ils publient, et doivent en assumer les conséquences, y compris sur le plan professionnel, dans un contexte où :

- La frontière entre le cadre professionnel et la vie privée est perméable sur les réseaux sociaux ;
- Il est possible d'identifier qui utilise un pseudonyme ou un « avatar », et de recouper les informations présentes sur différents réseaux sociaux (ex : contenus « professionnels » sur LinkedIn, contenus « privés » sur Facebook, hobbies sur des sites thématiques…) ;
- Les réseaux sociaux jouent un rôle d'amplificateur, où les contenus peuvent être repris ou relayés par des tiers.

Ainsi, même s'ils utilisent un « avatar » ou un pseudonyme, les Utilisateurs doivent veiller à :

- Ne pas utiliser leurs adresses de messagerie professionnelle, mais toujours utiliser une adresse personnelle ;
- Privilégier l'utilisation de mots de passe complexes, différents des mots de passe utilisés dans la sphère professionnelle ;
- Configurer les paramètres de confidentialité de leurs profils pour limiter les risques d'intrusion sur les plateformes de réseaux sociaux ou d'usurpation de leurs identités, penser à les vérifier régulièrement et réfléchir avant d'activer l'option de géolocalisation ;
- S'exprimer avec prudence, retenue et courtoisie et se comporter comme dans n'importe quel lieu social, avec les mêmes règles de savoir-vivre ; s'abstenir de tous propos et commentaires abusifs, injurieux, diffamatoires ou incitant à la haine ou à la discrimination ;
- Ne pas publier d'informations sensibles ou confidentielles relatives à la Société ou à ses clients, partenaires ou fournisseurs, ou toute information susceptible de porter atteinte au patrimoine de la Société ou à son image ;
- Ne pas se prévaloir de ses liens avec la Société ou mettre en avant ses fonctions pour appuyer ses publications ou contributions ;
- Ne publier que des images, photos libres de droit ou dont ils sont propriétaires ;
- Ne pas publier de contenus et ne pas citer de personnes sans disposer de leur accord préalable (respect de la vie privée, droit à l'image) et des droits adéquats (droits d'auteur, droit des marques…) ;
- Ne pas divulguer d'informations précises qui pourraient être utilisées à leur encontre, pour nuire à des tiers (famille, collègues…) ;

DG

- Ne pas publier ou relayer de fausses informations (faux avis, faux témoignages, dans le cadre de retweet par exemple…) et choisir avec soin avec qui partager un contenu.

Par exception, certains Utilisateurs peuvent être mandatés par leur hiérarchie pour s'exprimer sur certains réseaux sociaux au nom de la Société ou de leur service. Par défaut, les règles ci-dessus s'appliquent, sauf si une consigne différente est donnée en considération de la mission confiée.

5.6 Les services de stockage et de partage sur Internet

L'utilisation pour un usage professionnel de services sur internet non mis à disposition par la Société tels que des outils de stockage (par exemple et de manière non exhaustive OneDrive ou Google Drive), de rédaction communautaire, de partage collaboratif est interdite.

L'utilisation de solutions de visioconférence différentes de celles mises à disposition par la Société est tolérée en tant que participant, dès lors que les solutions fournies par la Société ne sont pas utilisables par les autres participants.

Même si l'accès à la ressource est possible, les Utilisateurs doivent faire preuve de vigilance lorsqu'ils téléchargent un fichier provenant d'une source externe.

Par exception, les projets collaboratifs conduits avec certains acteurs (tiers de confiance, entreprises partenaires…) pourront justifier la levée totale ou partielle des restrictions d'accès à ces outils, sous réserve de validation par le responsable de la sécurité des systèmes d'information.

DG

6. APPLICATION ET ÉVOLUTION DE LA CHARTE

La présente charte s'applique dès sa diffusion. Elle pourra être révisée en fonction des évolutions technologiques, règlementaires ou organisationnelles relatives du système d'information de la Société.

7. CONTACTS

RGPD – Délégué à la Protection des Données personnelles :
rgpd@dassault-aviation.com

Sécurité Informatique – Computer Security Incident Response Team :
csirt@dassault-aviation.com

* *
*