AÉROPORT
toulouse blagnac

CHARTE SUR L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
(Annexe au règlement intérieur)

Préambule

Au regard du rôle incontournable qu'exercent aujourd'hui les ressources informatiques et les télécommunications dans le fonctionnement de l'Aéroport de Toulouse Blagnac, la sécurité et la fiabilité de ces ressources doivent être une préoccupation majeure et permanente des utilisateurs.

Pour que tous puissent bénéficier pleinement de ces technologies tout en assurant leur bon fonctionnement, il est essentiel d'établir un équilibre approprié entre l'utilisation de ces ressources et la protection des intérêts de la société.

L'objet de la présente charte est d'informer les utilisateurs des modalités d'utilisation et de contrôle des ressources informatiques et des télécommunications de la Société ATB.

Elle précise à cet égard :

- L'ensemble des règles générales que chaque utilisateur doit respecter dans l'utilisation des ressources mises à sa disposition, de façon à assurer leur bon fonctionnement, leur sécurité et la protection des intérêts de la Société ATB,
- Les modalités des contrôles qui sont ou peuvent être effectués, dans le contexte de l'utilisation de ces ressources informatiques et télécommunications, afin que chaque utilisateur en soit informé.

Titre I – Champ d'application

1. Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, institutions représentatives du personnel, employés de sociétés prestataires, sous-traitants, et visiteurs occasionnels.

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

Des dispositions spécifiques sont prévues au titre VIII pour toute personne ayant un profil administrateur IT, entendu comme personne spécialement compétente en matière informatique, qui doit veiller à assurer le fonctionnement normal et la sécurité des ressources informatiques ou qui dispose de droits d'accès privilégiés sur tout ou partie du système d'information dont il n'est pas que l'utilisateur.

2. Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, réseaux informatiques (serveurs, routeurs et connectique), photocopieurs, réseau téléphonique (fixe, portable, DECT, fax, smartphone, tablette), logiciels, systèmes d'information partagés, fichiers, données et bases de données, systèmes de messagerie, services cloud, intranet, extranet, internet, wifi, abonnements à des services interactifs, vidéoprotection, visioconférences, partages de connexion, etc.

Titre II – Confidentialité des paramètres d'accès

L'accès au système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, et certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

L'utilisateur est personnellement responsable de l'utilisation qui peut être faite des paramètres de connexion qui lui auront été transmis.

Ces paramètres doivent être mémorisés par l'utilisateur et éventuellement stockés de manière sécurisée afin d'en garantir la confidentialité. En tout état de cause, ils ne doivent pas être transmis à des tiers ni notés sur papier libre. Ils doivent être saisis par l'utilisateur à chaque accès.

PC

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par les équipes en charge de la gestion du système d'information afin de recommander les bonnes pratiques en la matière.

A minima un mot de passe doit être d'une longueur minimale de 8 caractères, contenir au moins une majuscule, une minuscule, un chiffre et un caractère spécial. Ils doivent par ailleurs être changés tous les 3 mois.

Certains systèmes plus sensibles peuvent nécessiter une politique de mot de passe plus complexe et/ou des systèmes d'authentification à plusieurs facteurs impliquant par exemple le numéro de téléphone de l'utilisateur, une empreinte digitale ou une empreinte faciale.

L'utilisateur ne doit pas essayer de se connecter autrement que par les dispositions prévues par l'entreprise, il est interdit d'usurper l'identité d'une autre personne, y compris avec son accord.

En cas de perte ou de vol d'un élément identifiant, l'utilisateur s'engage à informer immédiatement son supérieur hiérarchique et les services de maintenance d'ATB.

Titre III – Protection des ressources sous la responsabilité de l'utilisateur

L'entreprise met en œuvre les moyens humains et techniques pour assurer la sécurité matérielle et logicielle du système d'information et de communication des outils mis à dispositions par ATB. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Les équipes de maintenance d'ATB sont responsables du contrôle du bon fonctionnement du système d'information et de communication. Ils veillent à l'application des règles de la présente charte en concertation avec le Responsable Sécurité des Systèmes d'Information. Les équipes de maintenance d'ATB sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.

Outre les exigences déjà énoncées, et en complément des mesures, l'utilisateur est tenu de :

- Sécuriser la session bureautique en verrouillant l'accès à son poste de travail dès lors qu'il s'éloigne de celui-ci et sans attendre la mise en veille automatique au bout du délai fixé ;
- Protéger systématiquement les documents sensibles ou confidentiels à l'aide de l'outil de chiffrement retenu par la société ATB ;
- Sécuriser le poste de travail si celui-ci est dans un espace public (fixe ou portable), en cas d'absence de l'utilisateur, dans un local / mobilier fermé à clé ou à l'aide du câble antivol fourni sur demande ;
- Ne pas connecter de périphériques personnels à son poste de travail ou au réseau ;
- Ne pas connecter d'outil de sauvegarde (clé usb, disque dur externe, en ligne, etc.) à son poste de travail sans avoir obtenu l'autorisation de la société ATB ;
- Ne pas installer de logiciels sans avoir obtenu préalablement une validation par ATB ;
- Ne pas connecter ou ne pas laisser connecter de postes de travail externes au réseau de la Société en dehors des moyens fournis par ATB pour y parvenir, notamment d'authentification renforcée.

L'utilisateur doit enregistrer ses fichiers dans les répertoires partagés ou dans son espace personnel « lettre U » dans les outils mis à disposition et sauvegardés par les services de maintenance d'ATB. Aucun fichier professionnel ne doit être stocké en local sur le poste de travail.

Titre IV – Accès à Internet

Dans le cadre de leur activité professionnelle, les utilisateurs ont accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par les services techniques d'ATB. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers et logiciels.

L'accès à Internet ne peut être utilisé dans le cadre d'une activité illégale. Il doit rester dans le respect de la législation en vigueur. Toute connexion à des sites à caractères injurieux, raciste, pornographique, pédophile, terroriste, diffamatoire, sexiste, discriminatoire, violent, négationniste, xénophobe, portant atteinte à la vie privée des personnes, ou à un droit de propriété intellectuelle-droit d'auteur est strictement interdite.

PC

Dans les espaces d'échanges (réseaux sociaux, forum, chat, blog, etc.), l'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs, et ne pas émettre d'opinions personnelles étrangères à son activité professionnelle, susceptibles de porter préjudice à la Société Aéroport Toulouse-Blagnac.

La communication sur les réseaux sociaux au nom d'ATB est strictement réservée aux personnes habilitées. Les communications des autres utilisateurs doivent donc être effectuées à titre personnelle.
La participation à des espaces de discussions professionnels via Internet nécessite l'accord des équipes de communication ATB car elle peut engager la responsabilité de l'entreprise.

L'utilisation de l'intelligence artificielle (IA) générative telles que ChatGPT, Gemini, Copilot, DeepL ou encore Perplexity est tolérée mais n'est pas recommandée au sein d'ATB.

En tout état de cause, il est strictement interdit d'envoyer ce type de données dans des IA :

- Des données classifiées de défense ;
- Des données classifiées diffusion restreinte ;
- Des données sensibles ;
- Des données personnelles (nom, prénom, coordonnées, etc.) ;
- Des données contractuelles, juridiques ou financières de l'entreprise ;
- Des secrets informatiques, comme des mots de passe ou des jetons d'authentification (clés d'API).

Les utilisateurs sont responsables de leurs actions et notamment de toutes malversations, dérives ou infractions commises qui ne se seraient pas conformé à ces règles.

Si la Société Aéroport Toulouse-Blagnac voyait sa responsabilité engagée à ce titre, elle pourrait engager toute poursuite et prendre toute sanction à l'encontre de l'utilisateur.

Titre V – Ressources informatiques

1. Dispositions générales

L'utilisateur doit enregistrer ses fichiers dans les outils mis à disposition et sauvegardés par les services de maintenance d'ATB. Aucun fichier professionnel ne doit être stocké en local sur le poste de travail.

Tout fichier ou courriel personnel devra être récupéré par l'utilisateur avant son départ. L'ensemble des éléments informatiques (compte, courriels, messagerie, etc.) seront supprimés a minima au bout de 1 mois et dans le délai maximal de 3 mois suivant le départ de l'utilisateur.

Les fichiers contenus dans l'ordinateur professionnel sont réputés avoir un caractère professionnel sauf si les utilisateurs les identifient comme étant personnels (mots clés pouvant être utilisés : « personnel », « perso » ou « privé »).
Tout dossier ou courriel ne portant pas cette identification pourra être récupéré et utilisé par ATB, la société disposant d'un droit d'accès en l'absence (temporaire ou définitive) de l'utilisateur.

ATB peut ouvrir et si besoin supprimer les fichiers identifiés comme personnels s'il existe un risque ou un évènement particulier (sécurité, sureté, atteinte aux règles de la présente charte) justifiant l'ouverture ou la suppression du fichier.

2. Dispositions spécifiques à la messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein de l'entreprise et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Des systèmes de sécurité analysent en permanence les mails envoyés ou reçus pour détecter du contenu frauduleux ou malveillant, auquel cas des dispositions sont prises pour les neutraliser, si nécessaire, en supprimant certaines communications.

Les utilisateurs sont invités à informer le support informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Tout doute sur la provenance et/ou contenu d'un message électronique doit faire l'objet d'une attention particulière et peut être envoyé à l'adresse mails-frauduleux@toulouse.aeroport.fr pour analyse.

PC

2.1 Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers.

Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir les informations transmises. Il convient également de s'assurer de l'historique des conversations communiquées le cas échéant.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires et ainsi respecter les dispositions relatives à la protection des données personnelles.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel ou en cas de données personnelles Il conviendra de veiller à ne pas transmettre de données personnelles sauf en cas de stricte nécessité.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception. Ils doivent, le cas échéant, être doublés par des envois postaux.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par les équipes de communication ATB notamment en ce qui concerne la mise en forme et la signature des messages.

2.2 Limites d'utilisation

Il est interdit d'envoyer un message (e-mail) à un nombre de personnes supérieur à 30. Les envois en plus grand nombre sont réservés aux services ou personnes habilitées.

Pour communiquer des informations syndicales ou indiquer des opportunités extra-professionnelles, des espaces sont mis à disposition sur l'Intranet ou sur les panneaux d'affichages.

Il est recommandé de ne pas envoyer de fichiers contenant des données personnelles. Toute transmission de données personnelles doit être strictement limitée et analysée afin de mettre en place les mesures de sécurité nécessaires, puis validée par les responsables de la données désignés par ATB.

Il est de la responsabilité de chacun de veiller à l'occupation de sa boite aux lettres de messagerie, afin de limiter tout risque de perte de messages dû à une saturation de celle-ci. Les utilisateurs doivent veiller à conserver les courriels contenant des données personnelles dans les limites des durées de conservation prévues dans l'entreprise.

Il est interdit de recourir à des procédures automatiques de renvoi de courriels à destination d'une messagerie externe.
En cas d'absence (temporaire ou définitive), il est recommandé d'activer le gestionnaire d'absence et d'indiquer l'adresse auprès de laquelle rediriger la demande. Pour la continuité de service, cette action pourra être menée par ATB, en l'absence de réalisation par l'utilisateur.

Tout salarié qui quitte l'entreprise définitivement verra ses droits d'accès clôturés au jour de son départ.

2.3 Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

PC

Les messages envoyés doivent être signalés par la mention " Privé " ou " Personnel " dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé " Privé " ou " Personnel ". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé " Privé " ou " Personnel ". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les utilisateurs sont invités à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de message à caractère personnel.

2.4 Recommandations et bonnes pratiques

Afin de s'assurer que les salariés s'approprient un bon usage des courriers électroniques et de lutter contre la surcharge informative, la Société Aéroport Toulouse-Blagnac souhaite rappeler les recommandations suivantes :

Être précis dans sa communication :

- Indiquer un objet clair pour tout message et correspondant au contenu du message ;
- Éviter de traiter plusieurs sujets dans un même message ;
- Signer un message afin d'être identifié rapidement (nom, prénom, fonction, coordonnées) en respectant la fiche de fonction et la charte graphique ATB ;
- Identifier son destinataire : madame, monsieur, prénom ; à défaut un mot introductif : « bonjour » ;
- Être courtois, utiliser les formules de politesse ;
- Utiliser modérément la couleur, le surlignement, la ponctuation excessive, les majuscules, le langage sms, les sigles et les smileys.

Limiter l'accessibilité « à tout prix » :

- Ne pas créer de sentiment d'urgence, se laisser et laisser aux autres le temps de répondre aux messages ;
- Raisonner par priorité ;
- Lorsqu'un message traite d'un dossier important et urgent, compléter l'envoi du message par des échanges directs (téléphone, face à face) ;
- En cas d'absence du bureau, actionner le « gestionnaire d'absences du bureau », paramétrer un message incitant à se rediriger vers un contact disponible, ou déléguer sa messagerie afin d'éviter les relances pour non-réponse ;
- Limiter l'envoi de messages en dehors des horaires de travail habituels afin de ne pas induire chez les destinataires un sentiment d'urgence à devoir répondre (hors périodes d'astreintes ou impératifs opérationnels). Sinon utiliser la fonction « envoi différé » ;
- Ne pas se connecter à sa messagerie durant ses temps de repos, ses congés ou durant les périodes de suspension de contrat (hors périodes d'astreintes ou impératifs opérationnels.

S'interroger sur la pertinence du média utilisé :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique au regard des autres outils de communication existants : face à face, téléphone, courrier,, visioconférence, outils collaboratifs ou de partage de documents, etc. ;
- Favoriser les échanges directs (téléphone, face à face) lorsque les niveaux de compréhension et d'interaction sont élevés, lorsqu'il y a un risque de mauvaise interprétation, lorsque l'échange devient conflictuel.

Ne pas abuser des pièces jointes :

- S'interroger sur la pertinence du (des) fichiers(s) à joindre au message.

S'interroger sur le(s) destinataire(s) principal(aux) du message :

- Cibler de façon précise le(s) destinataire(s) du message (« A » : pour action / « CC » : pour information) ;
- Utiliser avec modération les fonctions « copie conforme » et « copie cachée », ou privilégier une transmission spécifique aux destinataires « pour information » de façon à leur indiquer clairement le motif pour lequel vous souhaitez qu'ils aient connaissance du message ;
- Éviter les mails en cascades dans lesquels les expéditeurs commentent successivement, envisager si un échange direct n'est pas plus approprié.

Titre VI – Réseau téléphonique

Ce chapitre a pour objectif de définir les règles d'usage, les bonnes pratiques et les recommandations liées à l'utilisation des téléphones et smartphones professionnels mis à disposition des salariés de la société Aéroport Toulouse-Blagnac.

L'objectif est d'assurer une utilisation optimale, sécurisée et conforme à la réglementation en vigueur, tout en respectant les besoins professionnels et personnels de chacun.

PC

1. Mise à disposition

Les téléphones et smartphones professionnels ATB sont mis à disposition pour un usage avant tout professionnel selon la fonction occupée et les besoins identifiés. L'attribution est décidée par le service RH en collaboration avec les managers.

Il est rappelé que ces équipements demeurent la propriété de l'entreprise, et que leur utilisation doit rester conforme aux besoins liés à l'activité professionnelle. Toute utilisation non liée à l'activité de l'entreprise doit être maîtrisée, afin de ne pas nuire aux engagements de l'entreprise en termes de gestion et de conformité.

L'utilisation du smartphone hors Union Européenne n'est pas autorisée, sauf dérogation validée par la direction.

2. Recommandations et bonnes pratiques

2.1. Sécurité des données

- Utiliser 2 codes différents, complexes et difficiles à deviner (pas de combinaisons évidentes comme votre date de naissance ou "1234"), pour verrouiller son téléphone et sa carte SIM, ;
- Activer les fonctionnalités de sécurité proposées par l'appareil (reconnaissance faciale) ;
- Rester vigilant aux tentatives de phishing en particulier de liens, pièces jointes, QR Codes provenant de sources inconnues ;
- Les données personnelles présentes sur le smartphone sont de la responsabilité du salarié.

2.2. Cybersécurité

- Installer uniquement des applications disponibles dans les stores officiels (exemple : Apple store) ;
- Mettre régulièrement à jour le système d'exploitation et les applications pour bénéficier des derniers correctifs de sécurité ;
- Éviter de connecter son téléphone professionnel à des réseaux Wi-Fi publics non sécurisés (exemples : gares, aérogares, restaurant, hôtels) ;
- En cas de doute sur la sécurité d'une application ou d'un lien, contacter immédiatement le support informatique avant de poursuivre ;
- Ne pas partager ses identifiants ou mots de passe avec des tiers, même de confiance ;
- Ne pas stocker de données sensibles sur le smartphone et ne pas divulguer les informations confidentielles de l'entreprise via son téléphone professionnel ;
- Réaliser régulièrement une sauvegarde avec le logiciel d'entreprise (exemple : Itunes) pour assurer la récupération des données en cas de problème.

2.3. Utilisation en déplacement

- Respecter les règles de sécurité routière : l'utilisation du téléphone au volant est interdite, sauf en mode mains-libres ;
- Ne jamais laisser son téléphone sans surveillance dans des lieux publics.

2.4 Utilisation au bureau

- Répondre aux appels téléphoniques dès lors qu'une ligne individuelle est attribuée ;
- Activer la messagerie vocale ou le transfert d'appels en cas d'absence ou de rendez-vous, afin de garantir une prise en charge des communications ;
- S'isoler un maximum de ses collègues pour téléphoner avec son téléphone portable ;
- Régler le téléphone portable ou DECT en mode silencieux pendant les réunions ;
- Limiter l'usage du téléphone portable ou DECT durant les réunions.

pc

3. Règles d'usage

3.1. Confidentialité

- Veiller à ce que les conversations sensibles ne soient pas menées dans des lieux où elles pourraient être entendues par des tiers non autorisés.

3.2. Consommation de données

- Faire un usage raisonné des données mobiles mises à disposition, notamment pour éviter les dépassements de forfait ;
- Les communications téléphoniques (voix et data) à l'étranger en dehors de l'Union Européenne sont notamment interdites, sauf dérogation préalable et autorisée, afin d'éviter des surcoûts de hors forfait conséquents ;
- Les numéros composés depuis les postes téléphoniques de l'entreprise, ainsi que ceux des téléphones mobiles professionnels, sont enregistrés sur l'autocommutateur et figurent sur les factures détaillées.

3.3. Entretien et réparation

- Maintenir son téléphone professionnel en bon état ;
- En cas de problème technique, contacter immédiatement le service maintenance de l'entreprise.

4. Respect de la vie privée et du droit à la déconnexion

4.1. Droit à la déconnexion

- En dehors des heures de travail, vous n'êtes pas tenu de répondre aux appels ou messages professionnels (hors périodes d'astreintes ou impératifs opérationnels).

4.2. Surveillance et respect de la vie privée

- L'entreprise peut procéder à des vérifications sur les appareils professionnels pour s'assurer du respect de cette charte, mais s'engage à respecter la vie privée des salariés ;
- L'entreprise ne procédera à aucune géolocalisation de manière proactive, sauf en cas d'urgence, notamment en cas de vol de l'appareil ou pour des raisons de sécurité liées à l'utilisateur, comme dans le cadre du dispositif PTI (Protection du Travailleur Isolé).

5. Perte, vol et fin de contrat

5.1. Perte ou vol

- En cas de perte ou de vol de l'appareil, informer immédiatement son responsable et le service maintenance pour procéder à la désactivation, la réinitialisation et à la localisation du téléphone.

5.2. Restitution à la fin du contrat

- À la fin de son contrat ou lors d'un changement d'équipement, le téléphone professionnel doit être restitué en bon état. Toutes les données personnelles doivent être supprimées de l'appareil avant sa remise ;
- À la remise, le code de verrouillage du téléphone doit impérativement être communiqué pour permettre la réinitialisation de l'appareil.

Titre VII – Accès à distance

Afin de garantir la qualité et la continuité de l'activité de la Société Aéroport Toulouse-Blagnac, certaines fonctions nécessitent d'avoir un accès à distance à la messagerie électronique et/ou au téléphone professionnel.

De même, dans le cadre du télétravail, certains utilisateurs peuvent bénéficier d'accès élargis au système d'information.

PC

Les accès à distance ne peuvent être autorisés qu'après accord du Président du Directoire et/ou du service RH.

Les accès distants autres que pour le télétravail des salariés ATB doivent être encadrés par un contrat.
Les règles qui s'appliquent à l'accès à distance suivent les mêmes principes que celles relatives aux postes de travail et plus généralement à l'usage professionnel.

Outre les exigences déjà énoncées :

- Le télétravailleur est responsable des équipements qui lui sont confiés. Il doit en assurer la surveillance et la sécurité. L'utilisation des équipements est réservée au télétravailleur ATB et uniquement dans le cadre d'un usage professionnel ;
- Les télétravailleurs sont tenus d'installer et d'entretenir le matériel mis à disposition par l'entreprise ;
- La conformité des installations électriques, notamment en matière de normes électriques et de risques incendie, relève de la responsabilité du télétravailleur. Par ailleurs, le télétravailleur s'engage à respecter les règles d'utilisation fournies par les constructeurs ;
- Le télétravailleur ne doit pas se connecter aux réseaux wifi ouverts et non protégés qui peuvent permettre l'interception des échanges.

Le télétravailleur doit informer les services de maintenance d'ATB de toute anomalie qu'il aura constaté sur les équipements fournis.

Le matériel fourni par l'entreprise restant sa propriété, il devra être restitué sur le site d'ATB dès que l'utilisateur n'en n'aura plus besoin (fin du télétravail, suspension de plus de 6 mois ou rupture de contrat, etc.).

Par ailleurs, l'utilisateur ne pourra pas utiliser ce matériel pendant les périodes de suspension du contrat disciplinaire ou non médicale.

En cas de suspension longue durée, la société se réserve le droit de récupérer le matériel fourni par l'entreprise pendant la période d'absence de l'entreprise.

En mobilité :

Le Wi-Fi public dans des lieux fréquentés (exemple : cafés, centres commerciaux, restaurants, hôtels etc.) est interdit. Pour les autres Wi-Fi d'entreprise (exemple : entreprises partenaires, autres aéroports, etc.), nous encourageons les collaborateurs à utiliser systématiquement le VPN ou à défaut le partage de connexion via le téléphone d'entreprise.

Titre VIII – Dispositions spécifiques aux administrateurs de systèmes d'information

Les administrateurs de systèmes d'information (ci-après les « administrateurs ») peuvent selon leurs habilitations être affectés à un certain nombre de missions comme :

- La gestion, développement, l'exploitation, la communication et la maintenance du système d'information d'Aéroport Toulouse-Blagnac ;
- Le suivi et le contrôle de l'utilisation des ressources informatiques ;
- La mise en œuvre des logiciels et autres applications ;
- La gestion des anomalies et incidents ;
- La collaboration à la gestion des notifications des incidents de sécurité et des violations de données à caractère personnel, en lien avec le DPO (Délégué à la Protection des Données), le RSSI (Responsable de la Sécurité des Systèmes d'Information) et l'AQSSI (Autorité Qualifiée pour la Sécurité des Systèmes d'Information) ;
- Des actions de remédiation des systèmes d'information et de communication.

À cet égard, ils peuvent être amenés à avoir accès à certaines informations ou données d'autres utilisateurs, données présentant, par ailleurs, un caractère confidentiel.

Toute personne ayant des prérogatives d'administrateur est tenu de respecter les termes du présent titre.
Sont entendus comme administrateurs :

- Les administrateurs (SI) internes d'ATB.
- Les administrateurs (SI) externes, prestataires de services extérieurs.

Le rôle de l'Administrateur est de garantir le bon fonctionnement des systèmes et des réseaux d'ATB tout en veillant à la bonne qualité et continuité des systèmes d'informations. De fait, la maintenance préventive et curative, ainsi que le contrôle du niveau de sécurité du système d'information et de communication sont assurés par

PC

l'Administrateur. Il met également en œuvre la correction de toute anomalie des systèmes informatique. Enfin, il préconise et met en place des solutions de contournement permettant d'assurer la continuité des services.
Pour répondre à ses missions, l'Administrateur doit prendre connaissance et appliquer les bonnes pratiques de sécurité préconisées par ATB.

Sans que cette liste soit exhaustive, ses prérogatives sont détaillées ci-après :

- Prendre connaissance des informations des Systèmes d'Information ou y donner accès que dans le cadre des fonctions exercées et/ou sur demande explicite du (ou des) donneur d'ordre, dans le cadre de procédures formalisées ou dans les cas particuliers prévus par la loi ;
- Ne pas prendre connaissance de données personnelles d'utilisateurs, sauf sur demande formelle de l'utilisateur lui-même, et n'autoriser quiconque à y accéder, sauf cas particuliers prévus par la loi (par exemple, enquête judiciaire) ou habilitations formelles et légitimes notamment sur demande de la Direction ;
- Respecter les engagements de confidentialité et de non-divulgation ;
- Utiliser les informations exclusivement dans le cadre professionnel et des missions exercées ;
- Se connecter à une ressource du SI qu'après autorisation explicite de la personne à qui celle-ci est attribuée, notamment dans le cas de l'utilisation d'un logiciel de prise de main à distance sur un poste de travail utilisateur ;
- Documenter les actions et interventions structurantes de telle sorte qu'ATB ne soit pas dans un état de dépendance ;
- Ne pas abuser des privilèges, et limiter les actions aux ressources informatiques dans le respect de la finalité des missions confiées ;
- Ne pas prendre des consignes d'une personne non identifiée ou non habilitée à le faire et faire remonter au responsable hiérarchique toute requête paraissant inappropriée ;
- Ne pas contourner les procédures de sécurité établies, et en particulier ne pas prendre l'initiative de désactiver les mécanismes de contrôle d'accès et/ou de traçabilité, et ne pas porter atteinte à l'intégrité des fichiers de journalisation ou aux systèmes de supervision ;
- Utiliser exclusivement les logiciels validés par ATB dans le respect des licences acquises. Toute autre installation de logiciel doit faire l'objet d'une autorisation préalable de la maintenance ;
- Ne pas apporter volontairement de perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites ;
- Ne pas entreprendre d'actions pouvant menacer l'intégrité du système d'informations sans l'aval et l'autorisation expresse du responsable hiérarchique ;
- Saisir et informer le RSSI et l'AQSSI des manquements graves et caractérisées constatés résultant du non-respect de la charte informatique d'ATB ;
- S'assurer que toute demande de mise en place d'outils soit validée par le RSSI afin de respecter le niveau de sécurité requis ;
- Ne pas utiliser le serveur ou le système d'information d'ATB à des fins d'activités personnelles (ex : Création de sites ou répertoires…) ;
- Ne pas partager avec ses collègues ou divulguer à quiconque les codes nominatifs d'administration.

Titre IX – Données personnelles

1. Traitement de données personnelles par les utilisateurs

Les utilisateurs sont amenés dans le cadre de leur fonction à accéder à des données à caractère personnel. Ces données ont un caractère confidentiel.

En conséquence, conformément à la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'au règlement général sur la protection des données du 27 avril 2016 dit RGPD, les utilisateurs doivent prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin de protéger la confidentialité des informations auxquelles ils ont accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à les recevoir.

Si les collaborateurs sont amenés dans le cadre de l'exercice de leur mission professionnelle, à mettre en place un traitement de données personnelles (nouveau logiciel, collecte de données, prospection, newsletter, etc.). Il conviendra de vérifier préalablement la conformité du traitement ou se renseigner auprès du Délégué à la protection des données pour connaître les étapes à suivre pour mettre en œuvre un traitement de données conforme au RGPD

Les utilisateurs traitant des données à caractère personnel s'engagent notamment à :

- ne pas utiliser les données auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;

PC

- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de leurs fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- s'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de leurs fonctions, restituer ou supprimer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Les utilisateurs traitant des données à caractère personnel sont informés que toute violation du présent engagement les expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

2. Information des utilisateurs sur le traitement de leurs données personnelles

L'utilisateur est informé que les données à caractère personnel le concernant sont conservées par ATB pendant la durée de leur relation contractuelle et dans le respect des délais en matière de prescription.

Des mentions d'informations plus précises sont communiquées sur les différents traitements opérés selon différentes modalités : règlement, clause, affichage notamment. Une rubrique a également été créée sur Intranet avec un rappel des procédures mises en place et des bonnes pratiques.

L'utilisateur est informé qu'il dispose, pour des motifs légitimes, d'un droit d'accès, de rectification, d'opposition, droit à l'effacement, à la portabilité, à la limitation du traitement, relatifs à l'ensemble des informations le concernant.

Un Délégué à la Protection des Données personnelles (dit DPO ou DPD) a été désigné et a pour mission d'informer, de conseiller et de veiller au respect de la réglementation en matière de données personnelles. Il veille au respect des droits des personnes et peut être sollicité pour toute question à l'adresse suivante : dpo@toulouse.aeroport.fr.

Titre X – Contrôle des activités

1. Contrôles automatisés

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de vérifier le bon fonctionnement, assurer la sécurité et surveiller l'activité du système d'information et de communication.

Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs ;
- à l'utilisation d'internet (navigation web et autres services internet) ;
- à l'utilisation de la messagerie ;
- à l'utilisation des équipements informatiques, mobiles et des moyens de communication ;
- à la géolocalisation ;
- à la vidéosurveillance et à la vidéoprotection ;
- à la biométrie ;
- à la prévention de fuite de données.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler l'activité et les échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

2. Procédure de contrôle manuel

En cas d'anomalie constatée par les services de maintenance d'ATB, il peut être procédé à un contrôle manuel et à une vérification de tout équipement, donnée et/ou toute opération effectuée par un ou plusieurs utilisateurs.

Les équipes de maintenance d'ATB ont la possibilité de se connecter à distance sur tous les équipements sans que l'utilisateur en soit averti pour effectuer des opérations de maintenance, de contrôle et ou de configuration.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, les services de maintenance d'ATB ne peuvent ouvrir les fichiers identifiés par le salarié comme privés contenus sur les équipements mis à sa disposition par l'entreprise qu'en présence de ce dernier et après demande de la Direction.

PC

Par ailleurs, tout message envoyé ou reçu depuis la messagerie professionnelle est supposé avoir un caractère professionnel, sauf s'il est clairement identifié comme étant personnel (par exemple, avec l'indication "Personnel" ou "Privé" en objet) ou classé dans un répertoire "Personnel".

Un message identifié comme personnel est considéré comme une correspondance privée et l'employeur doit, sauf décision de justice, en respecter le secret.

Titre XI – Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés.

Cette responsabilité peut aussi être pénale et civile le cas échéant si l'infraction est prévue par le code pénal.

Titre XII – Numérique responsable

Pour réduire nos empreintes écologiques et concevoir un avenir numérique plus sobre et responsable, ATB s'engage pour limiter l'usage des technologies de l'information et de la communication. Des pistes existent comme la sobriété numérique qui consiste ainsi à modérer ses usages numériques quotidiens. Pour éviter la surconsommation numérique et inverser la tendance, voici quelques exemples de bonnes pratiques de sobriété à appliquer :

La gestion du matériel numérique :

- Recycler tout ce qui ne peut plus être ré-utilisé ou réparé (ex : cartouche d'encre) ;
- Éteindre les appareils qui ne nécessitent pas de fonctionnement permanent (notamment durant la pause déjeuner et la nuit) ;
- Diminuer la quantité des données stockées en les archivant et en les supprimant à fréquences régulière quand cela est possible.

La gestion des mails :

- Identifier clairement des destinataires pour limiter le nombre de mails envoyés ;
- Limiter l'option "répondre à tous" ;
- Trier sa boite mail et vider régulièrement la boîte « éléments supprimés » ;
- Se désabonner des nombreuses newsletters.

La gestion de l'impression :

- Limiter autant que possible les impressions via la digitalisation ;
- Régler des paramètres d'impression par défaut : recto/verso et noir et blanc ;
- Favoriser le déclenchement des impressions via un badge ou un code.

Titre XIII – Information des utilisateurs

1. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié par le biais de l'espace Intranet.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

Chaque utilisateur doit s'informer sur les bonnes pratiques et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

Les salariés seront formés pour appliquer les règles d'utilisation prévues par la présente charte. Ils trouveront notamment des documents d'information/formation en ligne sur l'intranet de l'entreprise, concernant la sécurité de leur poste informatique.

PC

2. Information des utilisateurs autres que salariés ATB

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

La présente charte peut en conséquence être annexée à un contrat avec un partenaire ou sous-traitant.

Titre XIV – Entrée en vigueur

La présente charte est applicable à compter du 1er janvier 2025. Elle a été adoptée après présentation en CSE du 20 décembre 2024.

Fait à Blagnac, le 1er janvier 2025

Pour la Société Aéroport Toulouse-Blagnac,

Le Président du Directoire,

Philippe CREBASSA