Charte informatique
de l'Aéroport de Bâle - Mulhouse

Charte de l'usage des NTIC

Préambule

L'Aéroport de Bâle-Mulhouse et notamment le service informatique a mis en place un système d'information et de communication qui comprend notamment un réseau informatique nécessaire à son activité.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder au système d'information et de communication mis à leur disposition et à les utiliser.

Toutefois, le système d'information et de communication de l'Aéroport est exposé en permanence à des risques importants menaçant son intégrité technique (virus, pannes).

C'est pourquoi, la présente Charte informatique pose les règles relatives à l'utilisation des ressources informatiques que chaque utilisateur s'engage à respecter.

Les collaborateurs de l'Aéroport doivent également être responsables et contribuer à la sécurité du système mis en place au sein de l'Aéroport.

De ce fait, la Charte informatique informe les collaborateurs de l'Aéroport des bonnes pratiques d'utilisation des ressources informatiques mises à disposition et des règles de sécurité à suivre ainsi que des moyens de protection mis en œuvre par l'Aéroport.

Toutes ces dispositions concourent au bon fonctionnement du système d'information et de communication et à la protection de la réputation de l'Aéroport.

Champ d'application de la Charte informatique :

La Charte s'applique à tout collaborateur de l'Aéroport, utilisateur des matériels et logiciels constituant le système d'information et de communication de l'Aéroport.

Elle s'applique aussi à toute autre personne exécutant un travail au sein de l'Aéroport et utilisant les matériels et logiciels du système d'information et de communication de l'Aéroport, quelle que soit la forme ou la durée de son intervention (personnel des entreprises extérieures et des sous-traitants intervenant à l'Aéroport, fonctionnaires et assimilés des administrations publiques, intérimaires, stagiaires...).

Le système d'information et de communication de l'Aéroport est notamment constitué des éléments suivants : ordinateurs fixes ou portables, tablettes, smartphones, téléphones, serveurs, logiciels, fichiers, données, bases de données et le système de messagerie.

SOMMAIRE

I. Contexte légal et réglementaire

L'Aéroport et la PSSIE	• Chaque collaborateur est soumis à la Politique de Sécurité des Systèmes d'Information de l'Etat Français (PSSIE). • La PSSIE est assortie d'exigences concrètes auxquelles la Charte se réfère.
Obligations des collaborateurs de l'Aéroport	• Les collaborateurs doivent utiliser les outils et ressources informatiques pour les besoins de leur mission professionnelle. • Toutefois, un usage exceptionnel à des fins personnelles peut être toléré par chaque responsable de service, mais cet usage ne doit en aucun cas entraver ni gêner l'exécution des missions du collaborateur et des tâches qui lui sont confiées. Au regard de la loi, le collaborateur peut engager sa responsabilité civile et/ou pénale lorsqu'il accède à des fins personnelles à un site internet contraire aux règlementations en vigueur et aux bonnes mœurs. Par conséquent, les responsables hiérarchiques se réservent le droit d'interdire toute utilisation d'Internet à des fins personnelles lorsque celle-ci présente un risque pour le bon déroulement de l'activité de l'Aéroport. • Chaque collaborateur s'engage à respecter les dispositions de la présente charte. A défaut, le collaborateur pourra s'exposer aux sanctions prévues par le Règlement intérieur.
Droit de regard de l'Aéroport	• Les dossiers et documents réalisés par les collaborateurs et stockés sur le réseau de l'Aéroport sont présumés professionnels, sauf mentions contraires. • Afin de protéger sa sécurité et sa réputation, l'Aéroport se réserve le droit d'analyser les données de trafic (données circulant sur le réseau et Internet) ainsi que les dossiers et documents stockés, dans le respect de la législation applicable. • Concernant les données à caractère privé, il appartient au salarié de procéder à leur stockage éventuel dans des fichiers explicitement prévus à cet effet et intitulés *«Personnel»* ou *«Privé»*. La protection et la sauvegarde régulière de ces données incombent au collaborateur. • L'Aéroport peut accéder aux fichiers identifiés comme *«Personnel»* ou *«Privé»* en présence du collaborateur ou d'un représentant du personnel, mais à la condition que le collaborateur ait été dûment et préalablement informé. • L'accès aux informations contenues dans les fichiers de journalisation (logs systèmes) est réservé aux administrateurs du système qui s'engagent à respecter la Charte Administrateur. La durée de conservation des fichiers de journalisation, directement ou indirectement nominatif, est de 1 an.

	• Ce délai peut être supérieur si un fichier est destiné à servir de preuve dans le cadre de règlement d'un litige ou d'une infraction.
Droit de contrôle de l'Aéroport	• La Direction de l'Aéroport se réserve le droit de contrôler le respect des dispositions de la présente charte. • Le contrôle est effectué au sein du service chargé de l'informatique par des personnes nommément désignées. Ce contrôle peut comprendre notamment un relevé de la durée de connexion à Internet, un relevé des sites Web visités, une analyse du format et de la taille des pièces jointes reçues ou envoyées.
Droit de sanction de l'Aéroport	• Le non-respect des règles et mesures de sécurité figurant dans la présente charte engage la responsabilité personnelle de l'utilisateur, dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables. Par conséquent, ce dernier pourra être exposé de manière proportionnée aux sanctions disciplinaires définies par le Règlement intérieur, eu égard aux manquements commis.

II. Information et participation des collaborateurs

Le visionnage de la Charte	La charte est consultable : • Pour les Utilisateurs Windows nommés et les stagiaires (ex : 'stageit') lors de la connexion à Windows. • Pour tous les Utilisateurs Windows communs, la charte sur la page intranet.
L'acceptation de la Charte	• Pour les Utilisateurs Windows nommés et les stagiaires (ex : 'stageit') : l'acceptation se fait par validation informatique lors de la connexion à Windows. • Pour tous les Utilisateurs Windows communs (ex : 'serviceaccueil') : l'acceptation se fait par signature de la version papier adressé par le Responsable de la sécurité des systèmes d'information (RSSI) et le document signé est retourné au RSSI.
La participation à la protection de la réputation et à la sécurité informatique de l'Aéroport	• Avec l'accord de sa hiérarchie, chaque collaborateur peut s'inscrire à une session de sensibilisation organisée par le service informatique. • Chaque collaborateur signale au CCO toute situation qui déroge à la Charte informatique et/ou qui concerne la protection des données à caractère personnel.

III. Les matériels et logiciels à utiliser ou à ne pas utiliser

Matériels à utiliser	• Les collaborateurs de l'Aéroport doivent utiliser **exclusivement** les ressources matérielles (ordinateurs fixes, ordinateurs portables, tablettes, smartphones, téléphones...) ainsi que les serveurs, les logiciels mis à disposition et configurés sous la responsabilité du Service informatique, les fichiers, données et bases de données, ainsi que le système de messagerie. L'adjonction d'un modem ou l'abonnement direct auprès d'un fournisseur d'accès internet sont formellement **interdits.** • Les équipements mis à disposition par l'Aéroport (connexion ou stockage d'objets) sont destinés à un usage professionnel ; un usage exceptionnel à des fins personnelles est toutefois toléré. • Si besoin, l'Aéroport permet l'utilisation par le collaborateur du disque D: de son ordinateur pour stocker ses fichiers privés (A noter qu'aucune donnée stockée sur les disques C : et D : n'est sauvegardée par l'Aéroport). • Les collaborateurs doivent utiliser les disques réseau (autres que D:) pour stocker les données professionnelles. Préconisations d'utilisation : - *«Personnel/Public»* : Documents professionnels personnels que vous partagez en lecture - *«Personnel/Privé»* : Documents professionnels personnels que vous ne partagez pas en lecture • Les collaborateurs ne doivent utiliser que des supports de stockage externe (Clé USB, disque dur externe, SD card...) à usage strictement professionnel, dont la source est certaine. • L'attribution des matériels et logiciels est faite dans le cadre de la *« Procédure d'attribution de ressources informatiques et de clôture »*, si nécessaire au travers d'une demande spécifique via le CCO. • Les collaborateurs doivent utiliser ces matériels et logiciels attribués avec soin.
Matériels à ne pas utiliser	• La connexion au réseau AÉROPORT (sauf à travers le hot spot *«Guest»)* à l'aide d'un matériel et/ou d'un logiciel non mis à disposition et configuré par le service informatique est **interdite.** • En cas de besoin, les collaborateurs doivent adresser au CCO leur demande de dérogation à cette interdiction. • Les collaborateurs ne doivent pas modifier intentionnellement la configuration d'un matériel ni d'un logiciel mis à disposition. • En cas de fonctionnement anormal, les collaborateurs doivent contacter le CCO.

IV. La gestion des droits d'accès aux applications

Droits d'accès aux applications	• Les droits d'accès aux applications sont gérés par les responsables de domaine applicatif, dont la liste est disponible au sein du système qualité.

V. La participation à la sécurité

Droits adaptés à la mission du collaborateur	• Pour des raisons de sécurité, les droits d'accès aux ressources applicatives externes (ex : sites web) et internes (ex : serveur, arborescence de fichiers) sont définis initialement, puis adaptés à la mission du collaborateur. • En cas de besoin d'évolution de ces droits d'accès, le collaborateur doit adresser sa demande, validée en amont par sa hiérarchie, au CCO. • Il peut être mis fin à l'accès à ces ressources lors de la cessation, même provisoire, de l'activité professionnelle du collaborateur. • Chaque collaborateur dispose d'un droit à la déconnexion dont les dispositions sont encadrées par une charte unilatérale sur le droit à la déconnexion datant du 11 janvier 2018.
Aucun accès aux Droits d'administration	• Pour des raisons de sécurité, les droits d'administration des matériels sont réservés au Service informatique. • En cas de fonctionnement anormal suspecté ou avéré, le collaborateur doit contacter le CCO.
Identifiants et Mots de passe non visibles	• Chacun est responsable de l'usage qui est fait de ses mots de passe. Les applications dont l'accès est gardé par mot de passe sont utilisées sous la responsabilité personnelle du titulaire du mot de passe, sauf usage frauduleux avéré par un tiers. • Les collaborateurs doivent choisir des mots de passe non triviaux et respectant le format éventuellement imposé par le service informatique. • Il est conseillé aux collaborateurs de changer régulièrement leurs mots de passe et de les garder strictement confidentiels. • En cas de nécessités de service, l'accès à la boîte de messagerie d'un utilisateur peut être ouvert à un autre collaborateur grâce à un paramétrage des boîtes de messagerie, ce qui évite la divulgation des mots de passe.
Nécessité de verrouiller les équipements	• Les collaborateurs doivent verrouiller leur poste informatique (mise en veille avec demande de mot de passe) en cas d'absence sur leur poste de travail ou lorsque l'appareil est hors de sa vue.
Accès des tiers	• Les collaborateurs ne doivent pas donner accès aux systèmes ou aux réseaux de l'Aéroport à des utilisateurs non autorisés.

	• L'accès d'un utilisateur aux informations et documents conservés sur les systèmes ou réseaux informatiques est limité à ceux qui lui sont propres, à ceux qui sont publics ou bien à ceux qui sont partagés. Par conséquent, aucune personne ne doit jamais essayer d'accéder, de copier, de modifier, de détruire des données ou informations (messages, fichiers...) appartenant à une autre personne sans son accord préalable.
Vigilance	• Chaque collaborateur doit signaler immédiatement au CCO toute tentative de violation de son compte ou de ses données personnelles ainsi que toute anomalie de fonctionnement.
L'utilisation d'une nouvelle application	• Chaque collaborateur doit se conformer au document *«Recommandations IT»* disponible dans le système qualité. En cas de difficultés, ce dernier doit contacter le Responsable Informatique.
Les obligations de chaque collaborateur en cas d'absence prolongée ou de fin de mission	• <u>Préalablement à son départ définitif et quelle qu'en soit la cause (fin de contrat, fin de mission...) l'utilisateur a l'obligation de :</u> - supprimer les répertoires ou documents *«Personnel»*, *«Privé»* au plus tard la veille de son départ. A défaut et sauf procédure judiciaire ou enquête administrative, ces répertoires sont automatiquement supprimés le lendemain du départ de l'utilisateur de l'Aéroport, sans être consultés et sans qu'aucune copie ne soit réalisée. - remettre à sa hiérarchie au plus tard à son départ, ou dans les plus brefs délais à la première réquisition de sa hiérarchie l'ensemble des moyens informatiques et de communication électronique, en bon état de fonctionnement, qui ont été mis à sa disposition dans le cadre de ses fonctions (ordinateur, téléphone mobile, cartes d'accès, moyens d'authentification à distance, badges, supports de stockage...).
Actes de malveillance informatiques	• <u>Il est formellement interdit :</u> - de perturber intentionnellement le fonctionnement des matériels et logiciels mis à disposition, ainsi que celui des systèmes informatiques de l'Aéroport. - de commettre intentionnellement un acte de malveillance informatique, quel qu'il soit, et ce, de quelque façon que ce soit, notamment par un usage anormal du matériel ou par l'introduction non autorisée de logiciels parasites (logiciels d'écoute réseau, virus, chevaux de Troie, bombes logiques...), sous peine d'être exposé aux sanctions disciplinaires prévues par le Règlement intérieur.

Dispositions légales	• Les collaborateurs ne doivent pas télécharger, copier, envoyer, ni utiliser des données ou des fichiers protégés par le droit d'auteur (MP3, vidéos, jeux, autres logiciels...). • Les collaborateurs ne doivent pas se connecter à des sites Web au contenu illicite ou contraire aux bonnes mœurs.

VI. Les échanges avec l'extérieur

Déontologie	• De façon générale, chaque collaborateur doit respecter les lois en vigueur et le principe de courtoisie lors de l'utilisation des ressources informatiques mises à disposition par l'Aéroport. • Aucun collaborateur ne doit diffuser des documents ou des correspondances à caractère diffamatoire ou injurieux, ou contenant des menaces explicites ou implicites, ou contribuant au harcèlement d'une personne de quelque nature que ce soit. • Aucun collaborateur ne doit charger, stocker, diffuser ou distribuer de documents, informations, images, vidéos à caractère illicite (pédophilie, racisme, nazisme, apologie du crime ou de la violence, terrorisme...) ou contraire aux bonnes mœurs (pornographie...), et ne pas solliciter l'envoi de tels documents. • Chaque collaborateur doit préserver l'image et la réputation interne et externe de l'Aéroport. • Mis à part la possibilité de diffuser un message sur les listes de l'Aéroport pour des raisons de service, aucun collaborateur ne doit envoyer des messages en masse. • Aucun collaborateur ne doit répondre aux messages en masse. • Tout collaborateur doit signaler au CCO tout élément informatique (ex : fichier, poste de travail, support de stockage externe...) suspecté de contenir un virus.
Données communiquées à l'extérieur	• Chaque collaborateur ne doit communiquer à l'extérieur de l'Aéroport que les informations minimales nécessaires afin d'éviter la divulgation d'informations confidentielles, susceptibles d'engager la responsabilité de l'Aéroport. Cette règle vaut quel que soit le mode de communication de l'information : mail, plateformes d'échange, supports amovibles...
Données reçues de l'extérieur	• Les données reçues sont susceptibles de contenir des virus infectant le poste du collaborateur, voire tout le réseau de l'Aéroport. Pour ce faire, le collaborateur ne doit utiliser que les plateformes d'échange de fichiers validées et mises à disposition par le Service Informatique. Chaque collaborateur ne doit utiliser que des supports de stockage amovibles issus de sources fiables. En cas de doute, ce dernier doit contacter immédiatement le CCO.

VII. Le service à contacter

Le CCO - Centre de Coordination (1010) à contacter	• <u>Le CCO doit être contacté :</u> - Lorsqu'un collaborateur suspecte que son poste est infecté, qu'il a des droits inhabituellement forts (administrateur du poste...) ou faibles, ou pour toute autre anomalie. - En cas de perte ou de suspicion de vol d'un équipement. - En cas de besoin d'évolution des droits sur les ressources internes. - Lorsqu'un mail a été mis en quarantaine par Mailcontrol et que le collaborateur se soit assuré de sa provenance. - En cas de questions sur la sécurité du système d'information.

VIII. La protection des données personnelles

Protection de données personnelles	• L'Aéroport attache une grande importance au respect de la vie privée de ses collaborateurs. • Toutes les opérations sur vos données à caractère personnel sont réalisées dans le respect des réglementations en vigueur et notamment de la loi n° 78-17 « Informatique et Libertés » du 6 janvier 1978 modifiée et du Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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. • <u>L'Aéroport conserve les données traitées pendant le temps nécessaire à la réalisation de la finalité des traitements concernés, notamment :</u> - pour l'exercice et la gestion de la comptabilité de l'entreprise, - pour la gestion de l'activité, de la prise de congés et de la rémunération du personnel, - pour l'organisation de sessions de formation par le personnel, - pour le remboursement de frais des besoins professionnels du personnel, - pour la gestion de l'utilisation du parc téléphonique de l'entreprise, - pour garantir la sécurité du système d'information, - pour garantir la sécurité et la sûreté aéroportuaire des biens et des personnes. • Les collaborateurs s'engagent à respecter une obligation de sécurité et de confidentialité adaptée aux données faisant l'objet d'un traitement dans le cadre de leurs activités.

Mise en œuvre d'un traitement de données	• Si le collaborateur doit être amené, pour l'exercice de sa mission professionnelle, à mettre en place un traitement de données personnelles (concernant par exemple les salariés, les clients), ce dernier devra au préalable en référer à son supérieur hiérarchique pour que ce dernier s'assure auprès du Délégué à la protection de données que le traitement est conforme aux lois applicables.
Exercice des droits des collaborateurs	• Conformément à la loi n°78-17 du 6 janvier 1978 modifiée et au Règlement (UE) 2016/679 relatif à la protection des données à caractère personnel applicable à compter du 25 mai 2018, tout collaborateur de l'Aéroport dispose des droits suivants sur ses données : droit d'accès, droit de rectification, droit à l'effacement, droit d'opposition, droit à la limitation du traitement, droit à la portabilité. Il est également possible de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. • Pour des motifs légitimes, tout collaborateur peut s'opposer au traitement des données le concernant. • Pour exercer ces droits, merci d'adresser votre demande, accompagnée d'une pièce d'identité au : Service Juridique, Aéroport de Bâle-Mulhouse, BP 60120, F-68304 Saint-Louis Cedex.

IX. Formalités légales/Date d'application/Publicité/Révision/Langues

Formalités légales	• La Charte informatique a fait l'objet de toutes les formalités légales obligatoires. Elle a notamment été soumise pour avis aux délégués syndicaux, au CSE et au CSP.
Application	• La Charte entre en vigueur le 01 avril 2018 pour une durée illimitée. • Elle annule et remplace à compter de cette date la précédente Charte informatique en vigueur depuis 2008.
Publicité	• La Charte informatique est communiquée contre récépissé à tout utilisateur de l'Aéroport et mise à disposition sur l'intranet de l'Aéroport.
Révision	• Elle peut à tout moment être modifiée ou révisée afin notamment d'être adaptée aux évolutions technologiques ou d'être mise en conformité avec l'évolution de la législation.
Langues	• La charte est établie en français et en allemand. En cas de contradiction entre ces deux versions, seule la version française fait foi, la version allemande étant une traduction de courtoisie sans aucune valeur juridique.

Fait à Saint Louis en 3 exemplaires, le 22 février 2018

Monsieur Matthias SUHR

Directeur

Monsieur Frédéric VELTER

Directeur Adjoint

Madame Elodie CAIZERGUES

Directeur des Ressources Humaines