1 Introduction

Le présent document fixe les droits et devoirs des personnes externes à l'ARRG qui interviennent dans le cadre d'un contrat de prestation SI sur des équipements techniques, industriels ou informatique de la plateforme aéroportuaire.

Dans cet objectif, l'ARRG demande à chacune des personnes intervenant dans le cadre d'un contrat avec l'ARRG d'adhérer à cette présente charte.

2 Objet

Cette charte décrit les comportements qui doivent être respectés afin d'assurer les conditions d'une maintenance correcte et sécurisée du système d'information de l'ARRG.

Elle a pour objet :

- De rassurer, la Direction de l'ARRG du bon respect de règles éthiques de la part des personnes en charge de l'installation et/ou de la maintenance du parc technique ;
- De préciser les principaux droits, les devoirs et les responsabilités des intervenants techniques ou informatiques externes.

3 Engagement

Tout intervenant technique ou informatique externe ayant une mission d'installation, de maintenance ou de réparation des ressources des systèmes d'information ou industriels de l'entreprise est tenue de respecter cette charte.

En cas de non-respect de cette charte, la SA ARRG peut prendre des sanctions administratives, dans le cadre de ses procédures applicables, et ceci sans préjuger des éventuelles poursuites judiciaires qui pourraient être initiées.

4 Définitions

- **Système d'information** : organisation des moyens humains et techniques permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et externes de l'entreprise, quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image ...).

- **Intervenant technique ou informatique externe** (ci-après Intervenant externe): Toute personne intervenant dans les locaux de l'ARRG pour installer, maintenir ou réparer un équipement informatique (systèmes ou réseaux) ou industriels. Cette personne doit être sous contrat direct ou indirect avec l'ARRG.

- **Administrateur d'un système d'information** : toute personne à laquelle a été confiée explicitement la responsabilité de la gestion technique d'un système informatique, d'un réseau, d'une application ou d'un sous-ensemble. Cette personne bénéficie des privilèges nécessaires et suffisants pour assurer les tâches de gestion confiées.

- **Utilisateur du système d'information** : toute personne autorisée à accéder, utiliser ou traiter des ressources du système d'information de l'ARRG dans le cadre de son activité professionnelle.

- **Ressource du système d'information** : l'information et ses différents moyens de partage, de traitement, d'échange et de stockage, l'ensemble étant la propriété de l'ARRG.

Toutes les récurrences aux « abus de droits et privilèges » renvoient à un usage ou détournement des informations auxquelles a accès l'administrateur, hors cadre de ses missions ou dans le but de nuire à des tiers ou à la SA ARRG.

5 Respect de la règlementation

L'intervenant externe doit

- Respecter strictement le secret professionnel lors du traitement d'information médicale et, le cas échéant, bancaire des salariés et clients de l'entreprise ou de toute autre information couverte par le secret (secret des affaires, secret industriel et commercial …) conformément aux réglementations en vigueur,
- N'utiliser que les seuls moyens de chiffrement mis à sa disposition par l'établissement *;*
- Respecter les règles de protection du droit d'auteur en ne se rendant pas coupable de contrefaçon, en particulier à l'occasion d'un téléchargement de données (marque, son, image, texte, logiciels, ...) depuis un site Internet ou en faisant une copie d'un logiciel commercial pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle ;
- Respecter les règles relatives à la protection des données à caractère personnel ;

L'intervenant externe ne doit pas, par l'abus de droit et privilège

- Utiliser ou détourner à son profit ou à celui d'un tiers tout ou partie du système d'information auquel il a accès, que ce soit ou non dans l'exercice de ses fonctions ;
- Porter atteinte, directement ou indirectement, aux systèmes de traitement automatisés des données, aux bases de données et aux logiciels : intrusion ou utilisation sans autorisation ;
- Intercepter des communications ou se livrer à la surveillance des autres postes de travail ;
- Divulguer les informations nominatives sans le consentement des personnes concernées.
- Divulguer les informations nominatives sans le consentement des personnes concernées.

6 Intervention à distance

Dans le cadre de ses activités liées aux contrats entre l'ARRG et l'entreprise qui l'emploie, l'intervenant externe peut être amené à intervenir à distance sur les équipements de l'aéroport. Dans ce contexte, et dans le strict respect des dispositions du contrat, notamment ses engagements de services et de délais,

L'intervenant externe doit :

- Respecter les procédures et modalités imposées par la SA ARRG afin de se connecter à distance et notamment :
    - Accès VPN,
    - compte nominatif pour chaque intervenant,
    - bastion d'administration de l'aéroport,

- Ouverture de l'accès à distance sur demande, quand exigé
- Authentifiant multi-facteur, quand exigé

- N'utiliser pour l'intervention à distance qu'un poste de travail avec un niveau de sécurité suffisant et respectant la politique de sécurité de la SA ARRG et notamment :
  - Poste muni d'un anti-malware à jour
  - Poste avec les dernières mises à jour critiques et de sécurité
  - Verrouillage du poste après un délai d'inactivité
  - Politique de mot de passe conforme aux préconisations de l'ANSSI pour la session de travail du poste
  - Restriction des composants logiciels, des processus et des services au strict minimum logiciels inutilisés
- Respecter scrupuleusement toutes les règles d'accès à distance qui lui seraient communiquées dans des circonstances particulières, notamment en cas de crise d'origine cyber ;
- Veiller à ne transmettre aucune information sur les données confidentielles à des tiers (y compris son entourage familial ou professionnel), à la seule exception des personnes identifiées au sein de son entreprise pour l'exercice du contrat avec l'ARRG ;
- Verrouiller l'accès de son matériel informatique et numérique afin de s'assurer qu'il en soit le seul utilisateur ;

L'intervenant externe ne doit pas, par l'abus de droit et privilège :

- Réaliser son activité professionnelle dans des conditions qui aggraveraient les risques usuels de vol de données par rapport à ceux éventuellement encourus au sein des locaux de l'entreprise ou du lieu de travail à distance ;
- Se connecter sur un serveur de l'ARRG à partir d'un ordinateur personnel au lieu d'un matériel fourni par l'entreprise ;
- Se connecter à un serveur de l'ARRG en utilisant un réseau Wifi public (café, restaurant, gare, train, aéroport...) ;
- Laisser son ordinateur professionnel connecté et accessible (non verrouillé) même pendant quelques instants.

7 Utilisation des moyens d'administration

Les exigences de cybersécurité de la règlementation ainsi que les mesures de traitement de certains risques imposent la mise en œuvre d'une architecture et d'une organisation spécifique pour l'administration de réseaux, des systèmes informatiques ou industriels sensibles. Dans ce contexte, les intervenants externes de l'ARRG respectent la bonne application des règles d'usage des moyens d'administration,

L'intervenant externe doit

- Respecter les procédures et modalités imposées par la SA ARRG afin de se connecter sur site et notamment :
  - Poste d'administration dédié et restant à demeure à l'aéroport, quand exigé,
  - Compte nominatif pour chaque intervenant,
  - Connexion au réseau mis à sa disposition (réseau filaire ou wifi)
  - Connexion via le bastion d'administration de l'aéroport, quand exigé,

  - En cas d'utilisation de clés USB ou de tout support de stockage de masse amovible, ces périphériques devront être vérifiés (analyse anti-malware) via la station blanche mise à disposition par l'aéroport avant toute connexion aux systèmes de l'aéroport
  - Authentifiant multi-facteur, quand exigé
- Utiliser un poste de travail qui dispose d'un niveau de sécurité suffisant et respectant la politique de sécurité de la SA ARRG et notamment :
  - Poste muni d'un anti-malware à jour
  - Poste avec les dernières mises à jour critiques et de sécurité
  - Verrouillage du poste après un délai d'inactivité
  - Politique de mot de passe conforme aux préconisations de l'ANSSI pour la session de travail du poste
  - Restriction des composants logiciels, des processus et des services au strict minimum logiciels inutilisés

L'intervenant externe ne doit pas, par l'abus de droit et privilège

- Connecter aux réseaux informatiques d'administration un poste de travail non autorisé pour l'administration des systèmes et réseaux sensibles ;
- Créer et utiliser un compte informatique autres que ceux existants, identifiés et autorisés aux tâches d'administration ;
- Utiliser les (identifiant, authentifiant) d'une autre personne (interne ou externe à l'ARRG) pour réaliser ses tâches d'administration ;
- Tenter de supprimer les traces d'activité d'administration des systèmes, réseaux et applications.

8 Surveillance des SI

L'ARRG a mis en place un bastion d'administration pour centraliser toutes les actions des administrateurs informatiques de l'ARRG et des prestataires se connectant sur le SI ARRG. Ce bastion permet:

- de contrôler les accès sur un point unique que ce soit pour des accès sur site ou à distance.
- De contrôler et d'enregistrer les actions (enregistrement des données saisies en ligne de commande, enregistrement vidéo des sessions bureau à distance). Ce contrôle permet de bloquer l'action ou prévenir l'administrateur ou le prestataire si l'action est jugée comme dangereuse ou pouvant porter atteinte au SI. Cet enregistrement permet également de vérifier les actions d'administration en cas de doute a posteriori ou pour des diagnostics d'incidents.

9 Gestion des incidents de sécurité

Un incident de sécurité du Système d'Information peut être considéré comme tout évènement potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve.

Dans ce contexte,

L'intervenant externe doit

- Examiner lors de ses interventions de maintenance les journaux d'événements de sécurité des applications, des serveurs ou des équipements industriels (si les fonctions existent) ;
- Conseiller sur la journalisation et l'archivage des événements de sécurité qui pourraient être révélateurs d'un incident de sécurité ;
- Notifier à la SA ARRG tout événement suspect ou incident de sécurité avéré.

L'intervenant externe ne doit pas, par l'abus de droit et privilège

- Créer , modifier ou supprimer les journaux d'événements (logs)
- S'accorder des privilèges dans une application ou un système jusqu'alors interdits sans accord préalable de la SA ARRG

Procès-Verbal d'Acceptation de la Charte SI des Intervenants Techniques ou Informatique externes de l'ARRG

Je soussigné

Nom :

Prénom :

Fonction :

Société :

Déclare avoir pris connaissance des éléments exposés ci-dessus et m'engage à les respecter dans le cadre de mes tâches d'installation, de paramétrage, de maintenance ou d'administration des équipements techniques, industriels ou informatiques de la SA ARRG.

Le : à Sainte-Marie

Signature précédée de la mention « Lu et approuvé» :