AÉROPORT LA RÉUNION ROLAND GARROS

LE VOYAGE COMMENCE ICI

SA Aéroport de la Réunion Roland Garros
97438 Sainte Marie

Clausier contractuel
–
Sécurité des Systèmes d'Information

AÉROPORT LA RÉUNION ROLAND GARROS

TABLE DES MATIERES

1. Définitions

Vulnérabilité : désigne toute faille, faiblesse, défaut de conception ou Programmes Malveillants affectant un produit ou un service SI.

Vulnérabilité majeure : désigne une Vulnérabilité, pouvant avoir des conséquences significatives sur un système d'information

Programme Malveillant : désigne un code informatique nocif tel que notamment virus, bombes logiques, vers, chevaux de Troie ou tout autre code ou instruction infectant ou affectant tout programme, logiciel, donnée, fichier, base de données, ordinateur ou autre matériel ou élément, endommageant, portant atteinte, compromettant l'intégrité ou la confidentialité, perturbant en tout ou partie le fonctionnement, détournant ou permettant de détourner en tout ou partie un système d'information de l'usage auquel il est destiné.

Incident : Un incident bloquant est un incident qui interdit l'utilisation du système, rendant impossible la continuité d'un ou des services proposés à la SA ARRG. Tous les autres incidents sont réputés comme non bloquants.

GTI : Garantie de temps d'intervention. Délai maximum au bout duquel le Titulaire intervient en cas de demande de la SA ARRG

GTR : Garantie de temps de rétablissement. Délai maximum au bout duquel le Titulaire résout un incident.

Dans la suite de ce document :

- Toute référence au « Titulaire » correspond au prestataire qui a été retenu par la SA ARRG,
- Toute référence à « SA AARG » correspond à la Société anonyme Aéroport Réunion Roland Garros.

2. Obligations générales de sécurité

D'une manière générale, le Titulaire est tenu de mettre en place les mesures techniques et organisationnelles nécessaires à la sécurité des données et du système d'information de la SA ARRG sur le périmètre qui le concerne, conformément aux règles de l'art et ce, afin d'assurer :

- Le maintien à un niveau de compétences en matière de sécurité des systèmes d'information suffisant à l'exécution des prestations.
- Le maintien des aptitudes requises pour couvrir les besoins sécurité de la prestation (qualifications, habilitations, certifications) et de pouvoir en justifier à première demande. Il doit par ailleurs attester d'une maîtrise suffisante des technologies requises et du savoir-faire nécessaire.
- La disponibilité, l'intégrité, la confidentialité des données et du système d'information de la SA ARRG sur le périmètre le concernant.
- La protection des informations de la SA ARRG contre toute divulgation, modification, destruction, perte, altération, accès, traitement accidentel, illicite ou non- autorisée.
- La traçabilité des opérations et des traitements effectués.
- La portabilité aisée des données dans un format structuré et couramment utilisé, sur demande de la SA ARRG et à tout moment, ainsi que la destruction de manière irréversible des données de la SA ARRG qui lui ont été transmises dans les conditions définies à l'Article « Réversibilité ».

Le Titulaire s'engage à justifier de la mise en place de ces mesures pendant toute la durée du Contrat, dans un délai de 72h suivant la demande de la SA ARRG.

Le Titulaire s'engage à respecter la Politique de Sécurité des Systèmes d'Information de la SA ARRG.

Le Titulaire se porte garant du respect de l'ensemble des dispositions relatives à la maitrise des risques liés aux systèmes d'information inclues dans le présent contrat par son personnel et par ses éventuels sous-traitants et partenaires. A cet effet, le Titulaire s'engage à mettre à la charge de son (ou ses) prestataire(s), partenaires ou sous-traitant(s) toutes obligations nécessaires, au moins équivalentes à celles prévues par le présent contrat.

Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage à informer la SA ARRG des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Le titulaire informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité ou une dégradation des performances du SI de la SA ARRG.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle doivent être pris en compte.

3. Obligation de confidentialité

L'ensemble des informations qui seront communiquées au cours des prestations restent confidentielles, elles ne peuvent faire l'objet d'aucune divulgation à des tiers ou à des membres du personnel du titulaire non appelés à participer à l'exécution des prestations, sauf si la divulgation est nécessaire en raison d'obligations légales, comptables ou règlementaires échappant au contrôle du titulaire.

A ce titre, le titulaire s'engage dès lors à signer un accord de confidentialité avant toute mise en œuvre des prestations. Celui-ci inclut entre autres, et sans que cela soit limitatif :

- Les modalités utilisées par le titulaire pour assurer la confidentialité et la sécurité des données transmises et produites dans le cadre du présent marché.
- La sécurisation, conservation, diffusion, accès, etc. de l'ensemble des éléments qui seront transmis
- La suppression et la destruction de tout ou partie des informations transmises et/ou produites de l'ensemble de ses systèmes à l'issue du marché (ou toutes versions physiques).
- La transmission d'un exemplaire de clause de confidentialité utilisé dans le cadre de ses contrats avec ses collaborateurs/salariés inclusion faite des cas de sous-traitance.

En outre, dès l'échéance ou la résiliation du contrat ou de la prestation, le titulaire doit cesser toute exploitation active des informations fournies par la SA ARRG, quelles qu'elles soient et s'engage à ne faire aucune rétention des documents ou fichiers appartenant à ce dernier. La SA ARRG s'engage à assurer la confidentialité des méthodes et du savoir-faire que le titulaire met en œuvre pour la réalisation des prestations qui lui sont confiées.

Le non-respect de cette obligation de confidentialité peut entrainer, outre les sanctions pénales éventuellement encourues, la résiliation du marché aux torts du titulaire sans que celui-ci puisse prétendre à une quelconque indemnité.

4. Obligation de Sécurité SI du Titulaire

6.1 Plan Assurance Sécurité

Dans le cadre du maintien en condition opérationnelle et de sécurité du système et/ou des prestations fournis, le titulaire devra compléter un Plan d'Assurance Sécurité.

Ce document contient l'ensemble des mesures de sécurité techniques, humaines et organisationnelles que le titulaire s'engage à mettre en œuvre à respecter et à maintenir tout au long de la prestation.

Le Plan d'assurance Sécurité complété et signé par le titulaire est annexé au contrat.

6.2 Protection des données de la SA ARRG

En raison de la sensibilité des données concernant la SA ARRG pouvant transiter au travers du système d'information du Titulaire, celui-ci attachera un soin particulier à assurer la sécurité physique et logique du système d'information traitant les informations de la SA ARRG.

Le Titulaire s'engage à assurer :

- La protection, la confidentialité, la disponibilité et l'intégrité de son système d'information et des informations de la SA ARRG ;

  Les mesures de sécurité mises en œuvre par le Titulaire devront être documentées, conformes aux règles de l'art applicables dans ce domaine, et adéquates, tels que des contrôles d'accès logiques et la mise en place de moyens de chiffrement des données de la SA ARRG conformes aux standards du marché afin d'empêcher l'accès à son système d'information à des personnes non-autorisées.

- La sauvegarde des informations de la SA ARRG de telle manière à permettre la restauration du service et des données.

- La conservation et le traitement des informations de la SA ARRG de manière séparée de ses propres données ou de données d'autres clients du Titulaire.

- La mise en place de dispositifs d'authentification et de vérifications des autorisations de toutes les personnes accédant aux informations de la SA ARRG via des contrôles d'accès logiques ;

- La communication à la SA ARRG, sur demande de celle-ci et sans délai, des traces (tels que les fichiers logs et évènements sécurité) et des analyses de sécurité le concernant, réalisées par le Titulaire pendant la durée du Contrat. La SA ARRG est d'ores et déjà autorisé à communiquer ces éléments aux autorités compétentes, sur demande de ces dernières ;

  Le Titulaire s'engage en outre à mettre en place une politique de traces destinée à garder de manière exploitable, sur une durée d'un an, la trace des actions réalisées et/ou tentatives d'actions dans son système d'information (notamment flux émis et reçus, nouvelles versions applicatives, tests, erreurs, les dé-doublonnages et les purges etc.) à des fins de contrôle (audit) et de preuves. Les traces comporteront à minima : nature, référence, identification de l'auteur de l'action et horodatage.

- La mise en œuvre, sous quarante-huit (48) heures à compter de la découverte d'un incident ou d'une menace pouvant affecter son système d'information, des mesures de sécurité renforcées adéquates ou toute solution permettant de répondre efficacement à l'incident ou à la menace.

Le Titulaire s'engage à justifier de la mise en place de ces mesures pendant toute la durée du Contrat, sans délai, sur demande de la SA ARRG.

6.3 Sécurité des matériels, logiciels et services fournis par le Titulaire

Le Titulaire s'engage :

- à ce que tous les matériels, logiciels et services objet du présent Contrat soient, dépourvus de toute vulnérabilité portant atteinte à la sécurité des systèmes d'information au démarrage de la prestation ;
- à mettre en œuvre un dispositif de veille en cybersécurité afin de détecter des vulnérabilités affectant les matériels, logiciels ou services fournis ;
- à informer la SA ARRG si des vulnérabilités sont découvertes sur les matériels, logiciels ou services fournis ;
- à mettre à disposition de la SA ARRG le correctif approprié dès que celui-ci est disponible chez les constructeurs et éditeurs.

Les matériels informatiques (serveur physique, switch, baie de stockage…) doivent disposer d'une garantie matérielle et d'un support constructeur permettant de bénéficier de remplacements et de réparations de matériels en cas de panne pendant au moins 3 ans à compter de de la livraison du matériel. Cette garantie pourra être renouvelée après la première période de garantie.

Les logiciels (Systèmes d'exploitation, logiciels informatiques, progiciels, firmware …) doivent être livrés avec un support permettant l'ouverture de tickets en cas de disfonctionnements. Les logiciels doivent être livrés avec une maintenance éditeur permettant de bénéficier de mises à jour logicielles fournies par l'éditeur.

Les modalités d'ouverture de tickets d'assistance ou de support technique devront être fournies à la SA ARRG au plus tard à la livraison des matériels et logiciels.

Si les services ou les dispositifs mis à disposition de la SA ARRG dans le cadre de ce projet contiennent des éléments cryptographiques, ces derniers doivent être conformes aux exigences de l'État en français en la matière :

- Les règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographiques. Annexe B1 du RGS 2.0
- La création, la distribution et la manipulation de clés cryptographiques. Annexe B2 du RGS 2.0

6.4 Programmes malveillants

Le Titulaire prendra toutes les précautions nécessaires pour éviter l'introduction de tout Programme Malveillant dans le système d'information de la SA ARRG et adoptera les mesures adéquates s'il constate l'existence d'un tel Programme Malveillant. A cet effet, le Titulaire réalisera tous les tests adéquats et s'engage à contrôler les éléments informatiques préalablement à leur livraison à la SA ARRG.

En cas d'introduction d'un tel Programme Malveillant, le Titulaire et la SA ARRG conviennent de collaborer afin d'en déterminer l'origine d'un commun accord et d'en éradiquer les conséquences.

S'il s'avérait que l'introduction du Programme Malveillant est imputable à la SA ARRG, celui-ci prendra à sa charge les frais de diagnostic et de remise en état.

S'il s'avérait que l'introduction du Programme Malveillant est imputable au Titulaire, celui-ci prendra à sa charge les frais de diagnostic et de remise en état.

En cas de désaccord entre les Parties un Comité de Suivi sera réuni.

5. Formation et sensibilisation en Sécurité des Systèmes d'Information :

Le personnel du Titulaire peut être amené à intervenir ou avoir accès à des systèmes ou à des données sensibles de l'aéroport.

Le titulaire s'engage ainsi à formaliser et suivre un programme annuel de sensibilisation et de formation en sécurité des systèmes d'information et en protection des données à destination de son personnel. Ce programme devra permettre :

- De réaliser une sensibilisation en sécurité des SI et en protection des données a minima annuelle pour l'ensemble de son personnel intervenant dans la cadre la Prestation objet de ce contrat. Le but est de fournir aux collaborateurs du Titulaire les bonnes pratiques sur des thématiques variées : hameçonnage, programmes malveillants, gestion des mots de passe, protection des clés USB, protection des données …
- De former son personnel de manière régulière afin de maintenir un niveau de compétences en matière de sécurité des systèmes d'information suffisant à l'exécution des prestations. Entre autres, le Titulaire doit former son personnel technique en charge de l'installation et de la maintenance des matériels, logiciels et services SI à la mise en œuvre de mesures de sécurité SI et au maintien en condition de sécurité SI.

Le titulaire s'engage également à collaborer avec la SA ARRG et fournir sur demande les éléments ci-dessous :

- Le programme de formation et sensibilisation en Sécurité SI
- Les éléments de preuves des formations et sensibilisation (attestations de formation, supports de formation, feuilles d'émargement…)

- Les indicateurs de suivi sur les formation et sensibilisation

6. Continuité d'activité

Plan de continuité d'activité :

Afin d'assurer une continuité de service des prestations dues à la SA ARRG, le Titulaire s'engage à

- mettre en place un Plan de Continuité de l'Activité (PCA) garantissant la continuité effective des services;
- soumettre son projet de PCA à la SA ARRG pour validation, avant sa finalisation et s'engage à prendre en compte les remarques et suggestions éventuelles de la SA ARRG justifiées au regard des contraintes réglementaires ou internes. Une fois ce PCA finalisé, le Titulaire s'engage à en assurer la gestion effective et le maintien opérationnel pendant la durée restant à courir du Contrat ;

Test régulier du plan de continuité d'activité :

Le Prestataire s'engage à tester annuellement le PCA (plan de continuité d'activité) selon un calendrier fixé avec l'aéroport. Ce test sera réalisé en concertation avec les équipes de l'aéroport. Le prestataire fournira un compte-rendu de ces tests à la SA ARRG. En cas d'échec des tests du PCA, le Prestataire s'engage, après exécution d'un plan d'action défini conjointement avec la SA ARRG, à exécuter un second essai et à en rendre compte à nouveau à la SA ARRG.

7. Réversibilité

Le Prestataire s'engage à assurer la réversibilité de la Prestation objet de ce contrat afin de permettre à la SA ARRG ou au prestataire choisi par la SA ARRG, de reprendre la gestion de cette Prestation. Le Titulaire s'engage à apporter l'assistance nécessaire durant la période de migration. Le Titulaire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

Par ailleurs, le Prestataire s'engage à restituer à la SA ARRG dans un délai maximal d'un (1) mois après la fin du Contrat, l'intégralité des Données dans un format conforme aux standards du marché et de manière à garantir leur intégrité, ainsi que les éventuels programmes, matériels ou autres logiciels, mis à la disposition du Prestataire par la SA ARRG dans le cadre du contrat.

Cette clause de réversibilité peut également être activée à tout moment avec un délai de prévenance d'un (1) mois et ce sans justification particulière. Cela peut se produire en cas de changement significatif de la situation du Titulaire (change d'actionnariat, délocalisation des sites d'hébergement…) ou de non-respect du Plan d'Assurance Sécurité.

La phase de réversibilité ne doit pas modifier la qualité, les termes et les conditions des services fournis durant le contrat.

8. Sous-traitance

Le Prestataire ne pourra pas sous-traiter tout ou partie des obligations qui lui incombent en vertu du Contrat sans l'accord préalable et écrit de la SA ARRG. En cas de sous-traitance autorisée, le Prestataire restera seul et unique responsable de la bonne exécution des Prestations. A cet effet, le Prestataire s'engage à mettre à la charge de son (ou ses) sous-traitant(s) des obligations, au moins équivalentes, à celles auxquelles il est tenu au titre du Contrat.

9. Engagements en cas d'accès, d'utilisation ou de gestion du SI de la SA ARRG par le Titulaire

14.1Utilisation du SI de la SA ARRG

Le titulaire s'engage à n'utiliser les ressources et les moyens de connexion au système d'information de la SA ARRG, mis à sa disposition par ce dernier, qu'aux seules fins d'exécution des prestations convenues au Contrat et dans le strict respect de la politique de sécurité du système d'information de la SA ARRG. A ce titre, il s'abstiendra de tout usage, communication, diffusion ou transmission de quelque manière que ce soit, d'informations confidentielles de la SA ARRG, telles que définies à l'article « Confidentialité » du Contrat, hors du système d'information de la SA ARRG sans l'autorisation de ce dernier, et ce quels que soient la cause, le motif ou l'objet.

Dans le cas où l'utilisation du SI de la SA ARRG nécessite l'usage d'un moyen d'authentification forte, le Titulaire respectera les procédures prévues par la SA ARRG pour la délivrance de ces moyens.

14.2Interventions sur site et à distance

Le titulaire s'engage à se conformer aux modalités imposées par la SA ARRG afin de réaliser les interventions sur site ou à distance.

Ci-dessous quelques mesures à respecter pour les accès à distance sur le SI de la SA ARRG (liste non exhaustive) :

- Accès VPN avec authentification via compte nominatif
- Connexion aux systèmes de l'aéroport via le bastion d'administration de l'aéroport
- Ouverture de l'accès à distance à la demande

Ci-dessous quelques mesures à respecter pour les interventions sur site (liste non exhaustive) :

- Le prestataire se connectera sur le réseau mis à sa disposition (réseau filaire ou wifi prestataire) et se connectera aux ressources à maintenir/administrer via le bastion d'administration de l'aéroport.

- En cas d'utilisation de clés USB ou de tout support de stockage de masse amovible, ces périphériques devront être vérifiés (analyse antivirus) via la station blanche mise à disposition par l'aéroport avant toute connexion aux systèmes de l'aéroport

10. Pénalités

En cas de non-respect par le Titulaire de ses engagements de services contractuels, la SA ARRG pourra le mettre en demeure de réparer ce manquement dans un délai d'une (1) semaine. A l'issue de ce délai, si le manquement n'est pas réparé, des pénalités pourront être appliquées à hauteur de 1% du montant global forfaitaire annuel de la Prestation par semaine de retard.

11. Résiliation

Dans le cas d'un manquement grave par le titulaire à l'une des obligations de sécurité SI mises à sa charge dans le présent contrat, la SA ARRG pourra le mettre en demeure de réparer ce manquement dans un délai de deux (2) mois. A l'issue de ce délai, si le manquement n'est pas réparé, la SA ARRG pourra résilier de plein droit le contrat.

Pour le Prestataire

Fait à :

Nom :

Fonction :

Signature et cachet :
*Précéder de la mention « **Lu et Approuvé** »*