**ANNEXE n°2 – Sécurite systéme d’information**

**I. Objet**

L’Annexe n°2 sécurité système d’information (ci-après « l’Annexe ») a pour objet de définir les conditions dans lesquelles le Titulaire s’engage à effectuer, dans le cadre du Marché auquel elle se rattache, pour le compte, sur instruction et sous l’autorité d’Inria, les opérations de Traitement définies ci-après (en II).

Dans le cadre de leurs relations contractuelles, les Parties s’engagent à respecter la règlementation en vigueur applicable à la sécurité des données.

**II. Description du Traitement faisant l’objet du Marché**

Le Titulaire devra assurer auprès d’Inria, tant au niveau individuel (chaque agent) qu’au niveau collectif (représentants de la direction, instances, groupes de travail) une fonction de conseil et de communication visant à :

* L’amélioration des conditions de vie et de travail dans les équipes et services ;
* L’hygiène générale des locaux de service ;
* L’adaptation des postes, des techniques et des rythmes de travail à la physiologie humaine ;
* La protection des agents contre l’ensemble des nuisances et les risques d’accidents de service ou de maladie professionnelle ou à caractère professionnel ;
* L’hygiène dans le restaurant administratif ;
* L’information sanitaire.

À cet effet, le médecin de prévention et/ou d’autres professionnels (ergonomes, psychologues du travail, ostéopathes, etc.) interviendront tant par des visites individuelles de surveillance médicale que par une action en milieu de travail et une participation aux actions collectives de santé ou de prévention.

La nature des opérations réalisées sur les Données est : collecte, enregistrement, organisation, conservation, adaptation, consultation, utilisation, effacement.

La Finalité du Traitement est : assurer les visites individuelles de surveillance médicale et participer aux actions collectives de santé ou de prévention.

La durée du Traitement correspondant à la durée du Marché.

Les types de Données Personnelles traitées sont : Nom, Prénom, Date de naissance, Numéro de téléphone personnel, Type de visite, Date d’embauche, Période d’essai, Catégorie de la visite, Intitulé du poste de travail.

**III : Exigences de sécurité d’Inria**

1. **Si transfert de données d’Inria vers le prestataire**

Inria mettra en place toutes les mesures de sécurité concernant la transmission des données vers le prestataire par l’utilisation d’outils adaptés (toutes les recommandations de sécurité citées ci-après son applicable chez Inria)

1. **Si le prestataire possède une plateforme qui permet à Inria de s’y connecter : Mode SAAS**

Celui-ci devra mettre en place toutes les mesures de sécurité citée ci-dessous

Un plan d’assurance sécurité (PAS) pourra être fourni au prestataire (Celui-ci se réfère aux exigences de sécurité)

Ou le prestataire fournira son propre PAS, si celui-ci possède une certification du type ISO 27001.

**Sécurité des données**

Le prestataire doit avoir mis en œuvre et documenté une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l’information au sein de son organisation.

Il doit notamment avoir nommé un responsable de la sécurité des systèmes d’information (RSSI ou toute autre personne exerçant cette fonction) et un responsable de la sécurité physique. Il devra communiquer les coordonnées de son RSSI (ou équivalent) à Inria.

**A noter que tout hébergement et transfert de données à caractère personnel d’Inria en-dehors de l’Union Européenne est proscrit par le RGPD.**

**Architecture de la solution**

Le respect de cette exigence est conditionné par le niveau de service demandé par Inria.

Le prestataire doit avoir mis en œuvre les redondances matérielles nécessaires pour fiabiliser l’architecture physique et ainsi se prémunir des pannes matérielles. Ces redondances interviennent à plusieurs niveaux. Par exemple :

* stockage (ex. : redondance disque, réplication sur une autre baie, etc.) ;
* serveurs physiques (ex. : clustering, déplacement automatique de machine virtuelle d’un hyperviseur à un autre, etc.) ;
* accès réseaux (ex. : redondance des accès, redondance du cœur de réseau comme le firewall ou les routeurs) ;
* alimentation électrique (ex : mise en place d’onduleurs électriques, redondance des alimentations électriques).

**Continuité d’activité**

Dans le cas où un plan de continuité d’activité (PCA) est demandé par Inria, le prestataire devra avoir mis en place et documenté un tel dispositif incluant les aspects de sécurité.

Le PCA devra notamment prévoir l’organisation et les mesures techniques prévues en cas de crise pour sécuriser l'activité maintenue afin d’assurer un niveau de service suffisant (éventuellement en mode dégradé, à définir avec la maîtrise d’ouvrage d’Inria).

**Reprise d’activité**

Dans le cas où un plan de reprise d’activité (PRA) est demandé par Inria, le prestataire devra avoir mis en place et documenté un tel dispositif incluant les aspects de sécurité.

Le PRA devra notamment prévoir l’organisation et les mesures techniques prévues suite à la survenue d’un incident majeur pour sécuriser la remise en activité de la solution.

**Accès à la solution par les utilisateurs Inria**

Le prestataire devra obligatoirement mettre en place des accès sécurisés à la solution. Par exemple :

* accès direct depuis un navigateur à l’aide de connexions type HTTPS ;
* accès grâce à un VPN ;
* accès via un portail dédié de type reverse-proxy ;
* tunnel chiffré type IPSec entre les infrastructures d’Inria et celles du prestataire

Des mesures de détection et de protection contre les tentatives d’accès illégitimes à la solution devront avoir été mises en place par le prestataire. Par exemple :

* limitation temporelle des connexions (augmentation du délai de façon exponentielle entre plusieurs tentatives infructueuses de connexion) ;
* blocage temporaire pour une certaine durée du compte après un seuil de tentatives infructueuses ;
* blocage du compte sur lequel une intrusion a été constatée et changement du mot de passe de l’utilisateur ;
* règles de composition des mots de passe à l’état de l’art ;
* détection de plusieurs connexions simultanées du même utilisateur depuis plusieurs adresses IP ;
* détection de plusieurs connexions simultanées d’utilisateurs différents depuis la même adresse IP si ce cas d’usage n’est pas prévu dans l’architecture mise en place ;
* génération d’une alarme en cas de tentative de connexion avec un compte fermé ;
* filtrage automatique ou non des adresses IP sources utilisées pour les tentatives d’intrusions ;
* détection de l’accès d’un utilisateur sans privilèges à des données hors du périmètre normal par exploitation des logs applicatifs détaillés ;
* génération d’une alarme en cas de détection d’un vol de session.

**Accès à la solution par d’autres applications (si nécessaire)**

Pour une bonne intégration de la solution dans l’ensemble du Système d’Information d’Inria la solution devra pouvoir s’interfacer avec d’autres applications de manière sécurisée (utilisation de protocoles sécurisés, utilisateurs applicatifs et de base de données possédant les droits strictement nécessaires, etc.).

Par exemple, concernant la mise à jour des profils ou des comptes applicatifs présents dans la solution, la solution devra pouvoir être pilotée par les interfaces de synchronisation avec le référentiel des comptes Inria.

Il en est de même pour la constitution et la mise à jour de la base infocentre d’Inria le cas échéant.

**Gestion du support utilisateurs**

Dans le cas où une prestation de support fera partie du contrat, le prestataire devra avoir prévu une politique de gestion du support (fonctionnel, technique, administration fonctionnelle) aux utilisateurs mentionnant notamment les aspects sécurité. Par exemple :

• quels outils et modes opératoires sont utilisés pour la prise de contrôle du poste utilisateur à distance ;

• des données à caractère personnel sont-elles manipulées par les équipes de support ;

• s’il y a lieu, quelles précautions sont prises par les équipes de support pour la manipulation de données à caractère personnel

**Documentation et formation**

Le prestataire fournira l’ensemble des documentations techniques et fonctionnelles pour décrire l’ensemble des points cités ci-dessus.

**Politique de sécurité de l’information et gestion du risque**

1 *Principes*

Le prestataire doit opérer la prestation à l’état de l’art pour le type d’activité retenu : utiliser des logiciels stables bénéficiant d’un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité optimal.

Il devra appliquer le guide d’hygiène informatique de l’ANSSI1 au système d’information du service fourni.

2 *Appréciation des risques de sécurité*

Le prestataire doit avoir réalisé et documenté une appréciation des risques de sécurité couvrant l’ensemble du périmètre du service fourni. Cette appréciation de risques devra être faite selon une méthode documentée garantissant la reproductibilité et comparabilité de la démarche (méthode EBIOS, Méhari ou autre).

Le prestataire doit, par exemple, prendre en compte dans l’appréciation des risques :

* la gestion de données d’Inria ayant des besoins de sécurité différents ;
* les risques ayant des impacts sur les droits et libertés des personnes concernées en cas d’accès non autorisé, de modification non désirée et de disparition de données à caractère personnel ;
* les risques de défaillance des mécanismes de cloisonnement des ressources de l’infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les commanditaires ;
* les risques liés à l’effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre commanditaires, en particulier lors des réallocations des espaces de mémoire et de stockage ;
* les risques liés à l’exposition des interfaces d’administration sur un réseau public.

Lorsqu’il existe des exigences légales, réglementaires ou sectorielles spécifiques liées aux types d’informations confiées par Inria au prestataire, ce dernier doit les prendre en compte dans son appréciation des risques.

Cette appréciation des risques doit être révisée régulièrement, au moins annuellement ou à chaque changement majeur pouvant avoir un impact sur le service.

**Sécurité de l’information**

*Classement et manipulation de l’information*

Le prestataire devra se conformer à l’échelle de sensibilité des données d’Inria pour la mise en œuvre des niveaux de classification de toute information liée au projet et procéder au marquage de cette information

*Protection des données*

Les données classifiées du projet devront être protégées par le prestataire. Par exemple :

* contrôle de l’intégrité des données (altération, suppression, perte, ...)
* détection d’un volume d’échange anormalement élevé qui pourrait être révélateur d’un incident de sécurité portant sur les données tel une exfiltration de données ou un accès illégitime à celles-ci ;
* signalement d’un privilège accordé à une population importante des administrateurs fonctionnels de la solution.

En cas d’incident sur les données du projet, le prestataire devra en informer rapidement le SOC d’Inria (cert@inria.fr) copie RSSI d’Inria (rssi@inria.fr) qui déterminera s’il y a eu – ou pas - une violation de données et si la DPO d’Inria (dpo@inria.fr) doit être prévenue.

*Suppression des données d’Inria*

Au terme du contrat liant le prestataire avec Inria ou en cas de rupture anticipée quelle qu’en soit la cause, ou à la demande d’Inria, l’intégralité des informations d’Inria devra être effacée conformément au délai prévu dans le contrat.

**Procédures d’exploitation documentées**

Les procédures d’exploitation du prestataire doivent être tenues à jour et accessibles au personnel concerné.

Une procédure de gestion des changements apportés aux systèmes en production doit exister et être documentée.

Cette procédure doit historiser tout changement ayant un impact sur la sécurité, avec, par exemple, les informations suivantes : date et heure programmées du changement, nature du changement, annonce lors du début et de fin de la mise en place du changement. Cet historique doit être communicable à Inria.

Un système de contrôle / historisation des versions du code source en production doit exister.

Les environnements de production doivent obligatoirement être séparés des autres environnements (tests développements, etc)

Des mesures de détection, de prévention et de restauration pour se protéger des codes malveillants doivent être mis en œuvre et des procédures ou formations appropriées de sensibilisation des équipes du prestataire mises en place.

Le prestataire doit avoir prévu et documenté une politique de sauvegarde de la solution fournie (informations, logiciels, configurations, etc.).

Un système de journalisation des événements doit être mis en place par le prestataire. Ce système de journalisation doit par exemple prévoir l’enregistrement des activités des utilisateurs (tant au niveau système qu’applicatifs et composants logiciels tels bases de données), les exceptions, les défaillances et les événements liés à la sécurité de l’information.

Les équipements de journalisation et les informations journalisées doivent être protégés contre les atteintes à leur disponibilité, intégrité, confidentialité ou traçabilité.

L’accès aux journaux doit être limité à un nombre restreint de comptes (seul ceux ayant besoin de l’information).

Un processus de veille et de supervision permettant la détection des vulnérabilités techniques de ses systèmes doit avoir été mis en place et documenté par le prestataire.

**Réversibilité**

Le candidat s’engagera à apporter l’assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par Inria, ou par un autre prestataire de service.

**Sécurité des opérations**

Des politiques, procédures et mécanismes de sécurité pour protéger toutes les opérations qui s’effectuent sur son système d’information doivent avoir été prévues et documentées par le prestataire, par exemple concernant :

* le traitement de l’information qui s’effectue sur les équipements de son système d’information, quel que soit leur type ;
* les échanges d’informations transitant par tous les équipements de télécommunication de son système d’information, quel que soit leur type.

**Prise en compte de la sécurité dans les développements**

Le prestataire devra intégrer dans ses développements les mesures techniques de sécurité nécessaires à la protection contre toute activité frauduleuse, toute divulgation ou modification non autorisée dans la solution lorsque celle-ci sera en exploitation par Inria.

Les équipes de développement du prestataire devront être en mesure de démontrer la mise en œuvre de mesures de sécurité en adéquation avec les exigences du projet.

**Relation avec des sous-traitants**

*Identification des sous-traitants*

Le prestataire devra répertorier l’ensemble des sous-traitants qu’il a identifiés comme participant à la mise en œuvre de l’offre (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance pour les tâches d’administration, etc.).

*La sécurité dans les accords conclus avec les sous-traitants*

En cas de recours à des sous-traitants, le prestataire devra reporter vers le(s) sous-traitant(s) concerné(s) des exigences de sécurité au moins équivalentes à celles qu’il s’engage à mettre en œuvre dans sa propre politique de sécurité, par exemple au travers d’exigences dans les cahiers des charges ou de clauses de sécurité dans les accords de partenariat. Ces exigences seront contractualisées.

*Gestion du changement avec les sous-traitants*

Dans la mesure où un changement de sous-traitant affecte le niveau de sécurité offert à Inria, le prestataire devra en informer Inria.

**Gestion des incidents liés à la sécurité**

*Responsabilités et procédures*

Le prestataire doit disposer de politiques et procédures documentées pour apporter des réponses rapides et efficaces aux incidents de sécurité. Celles-ci doivent définir les moyens de communication des incidents de sécurité aux clients concernés, et le niveau de sécurité exigé pour cette communication.

Les employés et sous-traitants doivent être informés de ces politiques et de ces procédures et les responsabilités et actions à réaliser doivent être clairement définies pour chaque acteur.

Ces procédures doivent notamment prévoir :

* d’alerter le SOC d’Inria (cert@inria.fr) dès toute suspicion de la survenue d’un incident de sécurité ;
* d’accuser réception dans les 24h à tout incident de sécurité de niveau critique signalé par Inria ;
* d’horodater dans un journal des événements l’ensemble des actions effectuées dans le cadre de la résolution de l’incident (indiquer au moins la date, l’action et les noms des intervenants ayant réalisé l’action) ;
* de présenter des points réguliers de la situation aux interlocuteurs d’Inria (chef de projet, service SOC, RSSI, DPO si incident RGPD) tout au long de la résolution d’un incident critique ;
* de prendre en compte le délai légal de 72h pour une déclaration à la CNIL par la DPO d’Inria dans le cas d’une violation de données personnelles pour fournir à la DPO d’Inria tout renseignements nécessaire (circonstances de l’incident, liste des personnes concernées, données exposées ou détruites, etc.) ;
* de présenter aux interlocuteurs d’Inria (chef de projet, service SOC, RSSI, DPO si incident RGPD) un bilan après résolution de tout incident de sécurité, même non critique ;
* de ne clore l’incident qu’après accord d’Inria lorsque l’incident ne concerne qu’Inria et pas d’autres clients.