

ANNEXE n°03 du CCAP – CLAUSES DE SECURITE

Obligations du Titulaire

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 l'IRD des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le Titulaire informe préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

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 encore l'évolution des techniques de compromission etc. doivent être pris en compte.

Comité de suivi

Le Comité de suivi sécurité, composé de membres de l'IRD et du candidat sélectionné, permettra de gérer la mise en place et l'évolution du volet sécurité de la prestation : respect du calendrier, conformité des prestations, respect de l'obligation de collaboration, validation des améliorations pour accroître la sécurité. Il peut être intégré à une instance de gouvernance déjà prévue au contrat telle que le comité de pilotage.

Il traite également des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations.

Application des plans gouvernementaux

Dans le cadre de l'application de plans gouvernementaux, le Premier Ministre peut décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications des opérateurs d'infrastructures vitales.

Dans le cadre du présent accord-cadre, le Titulaire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage (sans délais et en rendant compte du suivi à l'IRD) à appliquer les consignes de sécurité données par le donneur d'ordres. Ces mesures sont susceptibles d'évoluer. Les modifications sont régulièrement transmises durant l'exécution du présent accord-cadre.

Localisation des données

Lorsqu'une partie des exigences fonctionnelles est réalisée à partir d'un service en ligne du Titulaire, celui-ci est tenu de respecter les exigences suivantes :

- Les données devront être stockées sur le territoire national,
- Le Titulaire se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées.

Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.

En cas d'évolution, le Titulaire doit vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

Pour tout changement opéré ayant un impact sur la sécurité, le Titulaire doit communiquer 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.

Sécurité des développements applicatifs

Utilisation du cadre standard de développement : le Titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) de l'IRD comprenant notamment :

- L'organisation des équipes de développement et de la prestation ;
- Les configurations matérielles préconisées pour le développement ;
- Les outils de développement préconisés par l'IRD (logiciels, versions, etc.) ;
- Une structure de développement (framework) intégrant les fonctions de sécurité.

Propriété du code : l'IRD est propriétaire du code et des droits de propriété intellectuelle des éléments développés dans le cadre de la prestation.

Protection des codes sources : le titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.

Le Titulaire s'engage à respecter les procédures et moyens qu'il déploie lui permettant d'intégrer la prise en compte des règles et mesures de la PSSI dans la délivrance des prestations : organisation, méthodes de travail, procédures, outils, techniques, certifications, standards etc. ...

Sont également concernées les normes et méthodes employées pour prendre en compte la sécurité dans les développements, notamment :

- La gestion des risques dans le cycle de vie des développements ;
- La ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production et est responsable de leur mise en sécurité ;
- La prise en compte des besoins de sécurité dans le cycle de vie des développements, par exemple et selon les besoins et la nature des projets de développement ;
- La robustesse du code, le fonctionnement en mode dégradé (débit), portabilité ;
- Confidentialité : anonymisation des bases de tests, besoins de cryptage, gestion des habilitations ;
- Traçabilité ou gestion de la preuve ; toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure ;
- Intégrité : contrôles de saisie, contrôles de cohérence, contrôles aux limites, saisies de paramètres ;
- La sécurisation du code (p/r injection de code ...), les tests de code ;
- Le cryptage des bases et des échanges ;
- La maintenance à chaud ;
- L'organisation de tests et de la recette de sécurité ;
- La diffusion de correctifs et de patches.

Le Titulaire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre et notamment :

- Environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
- Contrôle rigoureux des entrées utilisateurs ;
- Sécurisation des accès aux fonctions d'administration ;
- Installation du minimum de fonctions nécessaires lors de l'installation ;
- Principe du moindre privilège ;
- Utilisation interdite de mots de passe dans le code ;
- Mise en œuvre d'une gestion efficace des erreurs
- Documentation du code : le titulaire doit commenter et documenter le code développé dans le cadre de la prestation. La documentation doit être mise à jour régulièrement.

Pour la mise en œuvre de technologies web, les développements pourront s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

La recette de l'application comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du Titulaire.

Personnels en charge des prestations

Le Titulaire est tenu de respecter le principe de l'individualisation des interventions : les comptes donnant accès à tout ou partie du système d'information de l'IRD auquel le Titulaire a accès doivent être nominatifs, et utilisés individuellement sans partage à des tiers.

Le Titulaire s'engage à tenir à jour et à communiquer à l'IRD la liste des intervenants avec les rôles et privilèges qui leur sont attribués. L'IRD se réserve la possibilité de faire réaliser une enquête par les autorités compétentes sur les intervenants.

Mobilité

Suivant la législation en vigueur, l'accès aux informations du Titulaire ou du client en situation de mobilité doit être encadré par des politiques et procédures spécifiques établies par le Titulaire et en corrélation avec celles du client, afin de prendre en compte les risques associés. En situation de mobilité, l'accès à ces informations doit être à un niveau de sécurité équivalent au niveau de sécurité de l'accès à ces mêmes informations hors situation de mobilité.

Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien...)

Le Titulaire s'engage à garantir l'effectivité des moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité du donneur d'ordres par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système du client. Cette exigence peut être étendue à tous les types de soutiens (ménage, chauffage, climatisation, etc) si la sensibilité du système le justifie.

Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec, etc.) garantissant la confidentialité et l'intégrité des données, en conformité aux règles et recommandations du RGS en la matière.