

TERME DE REFERENCE DE CONSULTANCE EXTERNE EN SECURITE INFORMATIQUE

I. Contexte :

Le Fonds d'intervention pour le développement (FID) s'étend actuellement dans 6 directions inter-régionales et une direction générale. Chacune dispose d'un parc informatique géré localement.

Le développement de ses activités à travers le volume toujours croissant des financements qui lui sont alloués incite le FID à investir davantage dans les infrastructures de la technologie IT. Ces extensions en termes d'utilisations de nouvelle technologie soulèvent le défi de faire face aux problématiques de la sécurité informatique, devenu incontournable pour une organisation de la taille actuelle du FID.

Pour y parvenir, le FID commence par le recrutement d'un consultant chargé de l'analyse et sécurisation du système informatique ayant pour objectif de diagnostiquer, d'auditer l'état de la sécurité du système informatique en général afin de dégager ensuite des recommandations.

Après plusieurs journées de travail acharnées sur bureau et sur terrain, plusieurs constats sont recueillis permettant de livrer des recommandations côtés matériels, logistiques, organisationnelles et humaines. Ces recommandations sont catégorisées suivant leur priorité et les budgets requis. Ils concernent globalement la mise en place des politiques de sécurités et la mise aux normes des équipements. La mise en place de ces recommandations requiert des expertises diverses dont une partie nécessite le renforcement de l'équipe informatique par le biais de recrutement de 03 consultants dont : un consultant externe pour le pilotage, un ingénieur sécurité informatique et un ingénieur système informatique pour la mise en œuvre et veille permanente.

Ce présent TDR décrira en détail la mission du consultant externe en système informatique pour la réalisation de l'une de pilier de la recommandation de la récente audit de la sécurité informatique

II. Objectifs de la mission

Suivant la recommandation de l'audit sécurité informatique, dans le cadre de la mise en place des standards et des normes de sécurité. Le FID fait appel à un consultant externe qui aura en charge d'appuyer la Direction Générale dans à la rédaction de la politique de sécurité (gouvernance), la conception et la mise place des outils nécessaire à la gestion et exploitation des systèmes informatique en général, ainsi que sa mise en œuvre, dont :

- Proposer une stratégie qui définira une feuille de route de sécurité, incluant l'analyse et l'évaluation des risques ;
- Accompagner le FID à veiller à ce que la politique de sécurité soit appliquée et assurer que les ingénieurs sécurité et administration du FID puissent prendre le relais;
- Proposer les outils de sécurité et de cyber protection les mieux adaptés aux FID ;
- Mettre en place un système de routines de fonctionnement des mesures de sécurité (un Plan de prévention des risques informatique et un Plan de continuité d'activité (PCA) ou Plan de maintien en conditions opérationnelles du SI (PCA/RAS)) ;
- Proposer des solutions afin de détecter les défaillances et proposer des actions correctives
- Planifier des audits de sécurité et suivre les plans de corrections
- Proposer les cahiers de charges pour les solutions de sécurité et les fournisseurs
- Participer à la formation des équipes IT et utilisateurs

A l'issue de sa prestation, le FID s'attend à ce que ses collaborateurs disposent d'un environnement informatique sécurisé et adapté à ses besoins pour qu'ils puissent mener à bien leurs missions. Ces conditions s'obtiennent par la réalisation de diverses étapes qui constitue des sous-étapes :

- Le FID dispose une politique de sécurisation des systèmes informatique pérenne ;
- Les outils de gestion et d'exploitation des systèmes informatique sont mis en place ;
- Le système de gouvernance de la sécurité informatique est mis en place ;
- Le FID est protégé contre les cyber-attaques des différentes sources ;
- Le planning d'audit et de maintenance sont établies ;
- Les personnels chargés de la veille sécuritaires sont en place et aptes à mener les interventions nécessaires ;
- Les matériels et les infrastructures adéquats sont en place ou leur spécificité technique bien défini
- L'équipes IT et les utilisateurs sont formés en matière de sécurité informatique.

III. Travaux à réaliser :

Le consultant est tenu à réaliser les prestations énumérées ci-après :

- Participer et définir à la gouvernance de sécurité du FID (politique, charte, stratégie, etc.)
- Accompagner le FID dans la modernisation de son réseau et de son système tout en assurant que les ingénieurs sécurité et administration recrutés puissent prendre le relais à l'issue de la prestation
- Définir et orienter le FID dans le choix de ses technologies et outils informatiques
- Piloter la configuration des équipements réseaux et sécurités (FW, Switch, Routeur, etc)
- Fournir une solution de télétravail
- Proposer la définition de la stratégie des privilèges et des droits des utilisateurs dans les systèmes
- Mettre en place les processus des normes et standards (change, incident, etc.)
- Conseiller le FID sur les bonnes pratiques à mettre en place pour sécuriser ses systèmes d'information (hardening et autres pratiques)
- Former les équipes sur la modernisation de l'architecture réseau et sécurité du FID
- Orienter le FID dans ces choix liés à son évolution informatique.
- Reporting constant à la DSI des situations de chaque projet de modernisation de l'informatique du FID
- Suivre les solutions répondant aux normes et standard ISO ;
- Documentation de site.

IV. Livrables :

Le prestataire est tenu de livrer au FID les produits suivants à titre de livrables :

- Un rapport détaillant la gouvernance de la sécurité des systèmes d'information du FID
- Les documents de procédure des bonnes pratiques des standards de sécurités (hardening)
- La réalisation des documents de procédure de change, d'incident et autres liés aux normes ISO
- Rapport de formation de l'équipe informatique en sécurité informatique sur les systèmes et solutions en place
- Une documentation globale de l'ensemble des systèmes d'information du FID
- Rapport de formation et des consultants internes

Ces livrables seront précédés d'une séance de restitution préalable.

V. Durée d'exécution de la prestation :

La durée de prestation est estimée à 90 HJ pouvant être répartis sur 6 mois suivant calendrier de recrutement des consultants interne et disponibilité des matériels de sécurité.

VI. Qualifications requises :

Profil demandé :

- Niveau de formation : Ingénieurs informaticiens (BAC+5) titulaires de diplômes délivrés par un établissement agréé ;
- Années d'expertise : minimum 10 années en sécurité informatique et 5 ans d'expériences dans l'administration des serveurs ;
- Ou ayant au moins réalisé 5 prestations similaire à l'offre.