REPUBLIQUE DU CAMEROUN

Paix - Travail - Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

REPUBLIC OF CAMEROON

Peace - Work - Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATION

RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.

MARCHE N° 0000038/M/MPT/SG/DAG/2021 DU 15/10/2021
PASSE APRES APPEL D'OFFRES NATIONAL RESTREINT N°00000026/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 LANCE EN PROCEDURE D'URGENCE POUR LE RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.

PLAN D'ACTION

Novembre 2021

Le prestataire	Visa ingénieur du marche	Visa chef service du marche

KÍAMA

DETAIL DU PLAN D'ACTION

LE PRESENT DOCUMENT EST LE PLAN D'ACTION POUR LA REALISATION DU MARCHE N° 00000038/M/MPT/SG/DAG/2021 DU 15/10/2021
PASSE APRES APPEL D'OFFRES NATIONAL RESTREINT N°00000026/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 LANCE EN PROCEDURE D'URGENCE POUR LE RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.

Ce plan d'action est établi en conformité avec l'article 23 du marché

SOMMAIRE

1. AVANT-PROPOS

Le présent document est confidentiel et sa confidentialité consiste à :

- La non divulgation des informations de configurations et paramétrages auprès de tierce partie ;
- La non reproduction des informations considérées confidentielles, sauf accord du Ministère des Postes et Télécommunications ;
- Les savoir-faire y contenus ne doivent profiter qu'au Ministère des Postes et Télécommunications ;
- Considérer toutes les informations déclarées Confidentielles.

2. Introduction et contexte

2.1. Contexte

De nos jours, les problèmes de sécurité informatique, de cybersécurité minent notre société. Depuis le décret n°2012/512 du 12 novembre 2012 portant réorganisation du ministère des postes et télécommunications, la Direction de la Sécurité des Réseaux et des Système d'Information a été créée afin de résoudre les difficultés liées à la sécurité informatique et cybersécurité sur l'ensemble du territoire national.

Selon l'analyse diagnostic faite dans le plan stratégique Cameroun numérique 2020, le volet « formation » est un problème qui entrave le développement des télécommunications et la marche vers le Cameroun numérique. Ceci est également le cas dans l'accomplissement des missions de la DSR en particulier et du MINPOSTEL en général. Au sein du Personnel, il n'existe pas de culture de la sécurité informatique, ni celle de la cybersécurité. Il y'a une inadéquation entre la formation initiale du personnel y travaillant et les missions qui y sont affectées.

2.2. Objet du projet

Le Ministre des Postes et Télécommunications lance un Appel d'Offres National Restreint pour le recrutement d'un Cabinet ou Bureau d'Etudes en vue du renforcement des capacités du personnel du MINPOSTEL en matière de cyber sécurité.

2.3. Consistance des prestations

Les prestations portent sur l'organisation de formation certifiante. Il s'agira donc concrètement de former le personnel du MINPOSTEL aux contenus en rapport avec le management des projets, la détection d'intrusion, l'identification, la protection, la riposte et la reprise après incident.

Chaque phase de cette formation (quatre au total) sera sanctionnée par un examen de certification pour évaluer l'assimilation et la mise en pratique des concepts appris.

Il s'agit des formations en Sécurité des systèmes d'information, certifications PMP (Projet Management Professional) et Cyber Security neXus suivantes :

- CSX | Fundamentals ;
- CSX | Practitioner.

3. Analyse de la situation et des lacunes

L'analyse de la situation a permis de faire les deux constats suivants :

1. Le nombre de personnes à former par certification n'est pas précisé dans les TDR ; il est vaguement dit qu'il s'agira de former le personnel du MINPOSTEL sans préciser les Directions concernées.
2. La participation aux formations proposées a un certain nombre de prerequis ; il est important de savoir dès l'entame de la mission quel est le profil des personnes qui seront formées.

Afin de bien mener la mission, il importe de corriger ces manquements en communiquant à KIAMA SA la liste des personnels à former ainsi que leurs profils de base afin que nous puissions les affecter efficacement dans chacun des modules de formation.

4. Buts et objectifs

La sécurité électronique est un enjeu majeur pour toutes les strates de la société et toutes les catégories de la population tant au niveau national qu'international. En quelques décennies l'espace numérique ou cyberespace est devenu un lieu de convoitise et d'affrontements pour les grandes puissances qui ont bien mesuré son caractère stratégique.

Le cyberespace se distingue dans les réalités traditionnelles par l'intangibilité des échanges qui s'y déroulent et l'interactivité entre les différents utilisateurs du réseau. Il a par ailleurs un caractère supranational qui, renforcé par l'autonomie du réseau internet n'y facilite pas l'application des principes juridiques traditionnels. De ce fait, de nombreux risques y naissent et rendent vulnérables toutes les entités qui le côtoient.

Conscient de ce qui précède, l'État du Cameroun a créé au sein de son Ministère des Poste et Télécommunications une Direction de la Sécurité des Réseaux et des Système d'Information. La mission assignée à cette Direction est de résoudre les difficultés liées à la sécurité informatique et cybersécurité sur l'ensemble du territoire national.

Seulement, toutes les analyses démontrent que la Direction de la Sécurité des Réseaux et des Système d'Information n'est pas suffisamment outillées en matière de compétences pour pouvoir répondre efficacement à cette mission. C'est dans le but de juguler ces écueils et de permettre à cette Direction d'exécuter sereinement ses missions que le présent projet vise à renforcer les capacités du personnel du MINPOSTEL en matière de sécurité électronique, de cybersécurité et de cyberdéfense afin d'assurer la sécurisation optimale du cyberespace Camerounais.

Il s'agira donc concrètement de faire former et inscrire aux examens de certification le personnel du MINPOSTEL. Les contenus seront en rapport avec la cybersécurité, le management des projets, la détection d'intrusion, l'identification, la protection, la riposte et la reprise après incident.

Au terme de notre prestation, les personnels désignés du MINPOSTEL seront outillés et passeront les examens de certification suivants :

- CSX Fundamentals : ce certificat teste les connaissances fondamentales en matière de cybersécurité dans cinq domaines :
    - Concepts de cybersécurité,
    - Principes de l'architecture de cybersécurité,
    - Cybersécurité des réseaux, des systèmes, des applications et des données,

- Réponse aux incidents,
- Sécurité de la technologie en constante évolution.

- CSX Practitioner : les aspirant doivent passer un examen qui démontre leur expérience en matière de pare-feu, de correctifs et d'antivirus, ainsi que leur capacité à mettre en œuvre des contrôles de sécurité courants, à effectuer des analyses de vulnérabilité et certaines analyses de réseau.

  A l'issue de la formation les participants devront avoir des compétences dans les domaines suivants :
  - Analyse des cyberattaques
  - Cybersécurité
  - Contrôles de cybersécurité
  - Gestion des changements informatiques
  - Pare-feux informatiques
  - Évaluation des vulnérabilités informatiques
  - Renseignements sur les menaces
- PMP : La certification PMP (Project Management Professional) est une certification internationale en management de projet. Cette certification est délivrée par le Project Management Institute. L'objectif de cette certification est de pouvoir évaluer formellement les expériences, connaissances et performances des chefs de projet à travers le monde et de faire reconnaître leur profession, comme activité substantielle aux projets.
- Les résultats attendus à la suite de la formation et de la certification sont :
  - La prise en compte de toutes les facettes de la sécurité dans l'élaboration des politiques de sécurité informatique et électronique ;
  - La conception des politiques de sécurité pertinentes capable d'être mis en œuvre ;
  - L'analyse des vulnérabilités et potentialités de sécurisation des infrastructures critiques ;
  - La modélisation des problèmes de sécurité des données, du matériel, et des réseaux ;
  - Assurer la veille technologique sur les évolutions en matière de risque et de parades ;
  - Convaincre les décideurs et les utilisateurs de l'importance des risques encourus et du bien-fondé des procédures envisagées ou déjà en cours ;
  - Préconiser et fournir des solutions équilibrées tenant compte des contraintes techniques, organisationnelles, relationnelles et financières ;
  - Respecter point par point une procédure de sécurité mis en place ;

- Organiser l'implémentation des décisions politiques, règlementaires et techniques auprès des utilisateurs ;
- Rédiger et proposer une charte d'utilisation des TIC en fonction des profils des différents utilisateurs.

Les livrables de cette mission sont :

ID	Livrables
L1	Le plan d'action du marché conformément à l'article 23 du contrat ;
L2	Le Planning détaillé du travail ;
L3	Rapport de la formation sur ISO 27001 LA ;
L3	Rapport de la formation sur CSX Fundamentals ;
L4	Rapport de la formation sur CSX Practitioner ;
L5	Rapport de la formation sur PMP ;
L6	Les justificatifs de paiement des vouchers permettant aux participants de passer les examens ;
L7	Le rapport global du projet.

5. Proposition d'une stratégie de mise en œuvre

Notre stratégie pour la réalisation de cette prestation est une démarche en cinq étapes qui sont :

Étape 1 : réunion de lancement

Le but est de Formaliser les objectifs de la mission, le planning prévisionnel des activités et les responsabilités de chaque partie prenante.

Étape 2 : préparation des formations

Au cours de cette phase, nous allons tenir des séances de travail avec le maitre d'ouvrage visant à clarifier tous les points d'ombre : nombre de participants, prérequis, profils, lieu, etc. puis nous allons adopter conjointement un plan de travail conforme à nos calendriers respectifs (disponibilité des participants et des experts).

En plus de ceci, nous allons préparer le site de formation (salles de formation, logement, logistique, etc.) et réserver les places et dates pour les examens.

Étape 2 : déroulement des formations

C'est au cours de cette phase que les formations proprement dites vont se mettre en œuvre.

Les formations se dérouleront de manière indépendante et pour les formations en sécurité informatique, la démarche consiste en un bootcamp intensif de 40 heures. Les participants travaillent avec le formateur chaque jour de 8h à 17h pendant cinq jours. Ils doivent par la suite réviser de manière autonome et se préparer pour la séance du lendemain.

A l'issue de chacune des phases de cinq jours, nous remettons aux participants des attestations justifiant de leur présence à la formation. De plus, tout le nécessaire pour la formation continue est mis à la disposition des apprenants : guides, livres, exercices,

simulateurs de questions, etc. Par ailleurs, des groupes whatsapp de suivi sont créés et les participants peuvent continuer de solliciter l'aide du formateur avant le passage proprement dit de l'examen.

Les domaines de formation seront ceux des curricula officiels de chacune des formations.

Étape 4 : examens de certification

Chaque participant à l'une des formations bénéficie d'un voucher lui permettant de passer l'examen de certification. Les participants reçoivent leurs vouchers et s'organisent librement pour passer leur examen. Le livrable pour nous étant la preuve d'achat de ce voucher.

Étape 4 : rédaction du rapport.

Il s'agit ici de rédiger le rapport définitif expliquant le déroulement intégral de la mission en y incluant les résultats obtenus.

6. Prochaines étapes de suivi proposés

Nous proposons le phasage suivant en sept étapes fondamentales pour le bon accomplissement de la mission :

- Du 18 octobre au 05 novembre 2021 : activités préparatoires

Il sera question ici de réaliser toutes les formalités nécessaires au lancement de la mission. Il s'agit entre autres de :

  - Prendre contact avec le Chef de Service du marché et l'Ingénieur du marché ;
  - Élaborer le plan d'action provisoire du marché (confère l'article 23, page 8).

- Du 08 novembre 2021 au 12 novembre 2021 : réunion de lancement.

Il s'agira de formaliser les objectifs de la mission, le planning prévisionnel des activités et les responsabilités de chaque partie prenante.

- Du 15 novembre 2021 au 19 novembre 2021 : préparation de la formation.

Il s'agira d'adopter un plan de travail conforme aux calendriers respectifs de disponibilité des participants et des experts puis de mettre en place la logistique de la formation : préparation du site, logement, réservations des vouchers….

- Du 22 novembre 2021 au 24 décembre 2021 : Formation

Les formations se dérouleront pendant 5 semaines à l'hôte Azur sis au quartier Bastos à Yaoundé. Nous mettrons à la disposition de chaque participant toute la documentation requise et le nécessaire pour la prise des notes. Pour chaque module de formation, un groupe whatsapp sera mis en place pour le suivi régulier des apprenants. Ces groupes seront actifs jusqu'à deux semaines après la fin de la formation et l'enseignant répondra à toutes les préoccupations dans un délai de 24h.

Nous allons commencer la première semaine c'est-à-dire du 22 au 26 novembre 2021 par les formations CSX Fundamentals et ISO 27001 Lead Auditor. Les formations se dérouleront en parallèle dans deux salles réservées à cet effet. Elles se dérouleront de 8h à 17h ; la pause-café et la pause déjeuner seront servies sur place. Les participants ne seront pas logés mais bénéficieront des indemnités de déplacement.

La semaine suivante sera consacrée à la formation en gestion des projets. Cette formation se déroulera en deux temps. Dans un premier temps, du 29 novembre 2021 au 03 décembre 2021, seront dispensés les enseignements en présentiel. Ces enseignements

se dérouleront selon les mêmes modalités que précédemment. A l'issue de ce temps, chaque apprenant recevra un compte de révision sur le simulateur d'examen PMP (https://www.project-management-prepcast.com/pmp-exam/the-pmp-exam-simulator) et pendant deux semaines, ils s'exerceront de manière autonome et pourront continuer à remonter leurs difficultés au formateur dans le groupe WhatsApp qui sera créé pour le suivi.

Les semaines restantes seront consacrées à la formation CSX Practitionner. La formation se déroulera également en deux temps : un premier temps de 05 jours pour la formation théorique et des TPs puis un accompagnement en distanciel pendant une autre semaine.

- Du 27 décembre 2021 au 31 décembre 2021: clôtures des formations.

Il s'agira ici de remettre les attestations de fin de formation aux participants ainsi que les vouchers d'examen.

- Du 03 janvier 2022 au 07 janvier 2022: Rédaction des rapports.

5 rapports seront produits : un rapport pour chacune des formations puis le rapport global de la mission.

- Du 10 janvier 2022 au 14 janvier 2022 clôture du marché.

Il sera question ici de rédiger et transmettre les livrables puis de procéder à la réception du marché.

7. Planning provisoire de réalisation du marché

		PHASE D'ÉVOLUTION DU PROJET (SEMAINES) S*0 = 15/10/2021*											
N°	**Activités**	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11	S12
1	**Activités préparatoires**												
1.1	Entretien préalable à l'exécution du marché avec le Chef de Service du marché et l'Ingénieur du marché												
1.2	Elaboration du plan d'action provisoire du marché (confère l'article 23, page 8)												
1.3	Transmission du plan d'action contenant le planning détaillé d'exécution du marché												
2	**Réunion de lancement**												
2.1	Formalisation des objectifs de la mission												
2.2	Validation du planning d'exécution du marché												
2.3	Validation des responsabilités de chaque partie prenante												
3	**Préparation des formations**												
3.1	Adoption d'un plan de travail conforme au calendriers respectifs de disponibilité des participants et des experts												
3.2	Réservation et préparation du site de formation												
3.3	Achat des vouchers permettant de passer l'examen de certification												
4	**Déroulement des formations**												
4.1	Formation à la certification la Certification CSX Fundamentals												
4.2	Formation à la certification la Certification CSX Practitioner												
4.3	Formation à la certification la Certification PMP												
4.4	Formation à la certification ISO 27001 LA												
5	**Clôture de la formation**												

5.1	Remise des attestations de fin de formation												
5.2	Remise des vouchers permettant de composer												
6	**Rédaction des rapports**												
6.1	Rédaction du rapport de la formation à la certification la Certification CSX Fundamentals												
6.2	Rédaction du rapport de la formation à la certification la Certification CSX Practitioner												
6.3	Rédaction du rapport de la formation à la certification la Certification PMP												
6.4	Rédaction du rapport de la formation à la certification ISO 27001 LA												
7	**Activités de clôture du marché**												
7.1	Élaboration et transmission du rapport d'exécution du marché												
7.2	Réunion de validation des recettes du marché												
7.3	Réunion de réception provisoire du marché												

Durée : 12 semaines.

ANNEXES

A1/ TERMES DE REFERENCES

I- Contexte et justification

De nos jours, les problèmes de sécurité informatique, de cybersécurité minent notre société. Depuis le décret n°2012/512 du 12 novembre 2012 portant réorganisation du ministère des postes et télécommunications, la Direction de la Sécurité des Réseaux et des Système d'Information a été créée afin de résoudre les difficultés liées à la sécurité informatique et cybersécurité sur l'ensemble du territoire national.

Selon l'analyse diagnostic faite dans le plan stratégique Cameroun numérique 2020, le volet « formation » est un problème qui entrave le développement des télécommunications et la marche vers le Cameroun numérique. Ceci est également le cas dans l'accomplissement des missions de la DSR en particulier et du MINPOSTEL en général. Au sein du Personnel, il n'existe pas de culture de la sécurité informatique, ni celle de la cybersécurité. Il y'a une inadéquation entre la formation initiale du personnel y travaillant et les missions qui y sont affectées.

II- Objectif du projet

L'objectif global est de renforcer les capacités du personnel du MINPOSTEL, en matière de sécurité électronique, de cybersécurité et de cyberdéfense afin d'assurer la sécurisation optimale du cyberespace Camerounais.

Il s'agira donc concrètement de faire former et certifier le personnel du MINPOSTEL, les contenus seront en rapport avec la cybersécurité, le management des projets, la détection d'intrusion, l'identification, la protection, la riposte et la reprise après incident.

III- Résultats attendus du projet et indicateurs de rendement

L'impact global recherché est la sécurisation optimale du cyberespace du Cameroun. Quant aux effets, ce sont les changements d'attitudes et de comportements de l'ensemble du personnel vis-à-vis des problématiques de sécurité informatique et électronique, mais aussi de limiter, par le respect des règles mises en place, l'exposition des Institutions aux menaces informatiques. Ce qui se traduira dans les faits par plusieurs éléments mesurables ou produits. Une approche plus globale de la sécurité qui se matérialisera par :

- la prise en compte de toutes les facettes de la sécurité dans l'élaboration des politiques de sécurité informatique et électronique ;
- la conception de politiques de sécurité pertinentes et capables d'être mise en œuvre ;
- L'analyse des vulnérabilités et potentialités de sécurisation des infrastructures critiques ;
- la modélisation des problèmes de sécurité des données, du matériel, des réseaux ;
- Préconiser et fournir des solutions équilibrées tenant compte des contraintes techniques, organisationnelles, relationnelles et financières ;
- Convaincre les décideurs et les utilisateurs de l'importance des risques encourus et du bien-fondé des procédures envisagées ou déjà en cours ;
- Organiser l'implémentation des décisions politiques, réglementaires, techniques (concernant la sécurité informatique et électronique) auprès de tous les utilisateurs ; Rédiger et proposer une ou des chartes d'utilisation de TIC en fonction des profils des différents utilisateurs ;
- Assurer une veille technologique sur les évolutions en matière de risques et de parade.

- Respecter point par point une procédure de sécurité informatique mise en place ;

IV- Méthodologie du projet

La mission du Prestataire s'articule autour de trois phases principales :

- Avant le début de ses prestations, il aura pris soin de finaliser son plan de travail, la méthodologie utilisée et le calendrier de son intervention. Au préalable, il aura obtenu du Maître d'Ouvrage toute la documentation nécessaire pour l'accomplissement de sa mission ;
- Pendant la mission, le Prestataire mènera des enquêtes auprès des différents acteurs en vue de recueillir leur opinion sur l'efficacité des mesures envisagées ;
- Au terme de sa mission, le prestataire soumettra un rapport dans les délais et en conformité avec les dispositions des présents termes de référence.

V- Chronogramme d'exécution

Les formations proposées dans le cadre du présent projet se dérouleront selon le chronogramme suivant :

CHRONOGRAMME D'EXECUTION					
PHASES	**TACHES**	**M1**	**M2**	**M3**	**M4**
Formation à la certification la Certification CSX Fundamentals	Cours, évaluations, TP				
	Examen de certification				
	Atelier de restitution				
Formation à la certification la Certification CSX Practitioner	Cours, évaluations, TP				
	Examen de certification				
	Atelier de restitution				
Formation à la certification la Certification PMP	Cours, évaluations, TP				
	Examen de certification				
	Atelier de restitution				
Formation à la Sécurité des systèmes d'information	Cours, évaluations				
	Atelier de restitution				

VI- profil du consultant

La mission sera confiée à une Institution national agréé (également par ISACA) justifiant d'une expérience en matière de cyber sécurité, de la lutte contre la cybercriminalité, la sécurité des réseaux et des systèmes d'information. Le consultant devra par ailleurs disposer de compétences avérées dans l'élaboration des politiques de sécurité des systèmes d'information.
L'équipe devra être composée d'experts de la manière suivante :

- Un (01) chef de mission de nationalité camerounaise, ingénieur expert en sécurité des systèmes d'information, (BAC +5 au moins en sécurité des systèmes d'information ou domaine connexe, certifié manager de sécurité des systèmes d'information et /ou PMP). Il devra justifier d'au moins cinq (05) ans d'expérience en sécurité des systèmes d'information ou cybercriminalité, parler et rédiger couramment le français ou l'anglais ;

- Un (01) ingénieur expert en réseaux de communications électroniques (BAC+5 au moins en télécommunications, certifié en CSX Fundamentals, CSX Practitioner avec au moins cinq (05) ans d'expérience en sécurité des systèmes d'information, ayant une expérience avérée dans la formation. Il doit parler et rédiger couramment le français ou l'anglais ;
- Un (01) Ingénieur en informatique (BAC +5 au moins en informatique, certifié en audit ou sécurité des S.I. - CISA et/ou CISSP de préférence) avec au moins cinq (05) ans d'expérience en sécurité des systèmes d'information. Il doit parler et rédiger couramment le français ou l'anglais, avoir des connaissances dans le domaine de la sécurité informatique et la protection de l'information ;

Le consultant indiquera de manière claire et précise la composition de l'équipe chargée de réaliser cette mission. Il y a lieu de préciser qu'en aucun cas, le profil de l'intervenant remplaçant ne saurait être inférieur à celui de l'intervenant remplacé.

VII- budget et financement

Le projet sera financé par le Fonds Spécial des Activités de Sécurité Electronique (FSE) du Ministère des Postes et Télécommunications, exercice 2021.