|  |  |  |
| --- | --- | --- |
| **REPUBLIQUE DU CAMEROUN**  **Paix - Travail - Patrie**  **----------------------** | C:\Users\DELL\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo MINDCAF.PNG | **REPUBLIC OF CAMEROON**  **Peace - Work - Fatherland**  **------------------** |
| **MINISTERE DES POSTES ET TELECOMMUNICATIONS**  **------------------** | **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.**

**RAPPORT DE LA FORMATION SUR CSX PRACTITIONER**

**Novembre 2021**

**RAPPORT DE LA FORMATION SUR CSX PRACTITIONER**





LE PRESENT DOCUMENT EST LE RAPPORT DE LA FORMATION SUR LE MODULE CSX PRACTITIONER DANS LE CADRE 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.

Tous droits réservés. Aucune partie de ce document ne peut être reproduite, mise en mémoire dans un système de recherche bibliographique ni transmis sous quelque forme ou par quelques procédés que ce soit électronique, mécanique, par photocopie ou autres sans autorisation préalable. Adresser une demande motivée, en indiquant les passages ou illustrations en cause au MINPOSTEL maitre d’ouvrage de cette étude susmentionnée.

**SOMMAIRE**

[**1.** **AVANT-PROPOS** 6](#_Toc90284431)

[**2.** **Introduction et contexte** 7](#_Toc90284432)

[**3.** **Objectifs de la formation** 9](#_Toc90284433)

[3.1. Objectif général 9](#_Toc90284434)

[3.2. Objectifs spécifiques 9](#_Toc90284435)

[**4.** **Méthodologie choisie** 10](#_Toc90284436)

[**5.** **Déroulement de la formation** 11](#_Toc90284437)

[**6.** **Domaines abordés** 13](#_Toc90284438)

[**7.** **Conclusion** 14](#_Toc90284439)

[ANNEXES 15](#_Toc90284440)

[A1/ ATTESTATIONS DE PARTICIPATION 16](#_Toc90284441)

[A2/ LISTES DE PRESENCE 17](#_Toc90284442)

[A3/ PHOTO DE FAMILLE 22](#_Toc90284443)

# **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.

# **Introduction et contexte**

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 d’apporter un début de solution à ces problèmes que le marché « N° 0000038/M/MPT/SG/DAG/2021 DU 15/10/2021 passé après appel d’offres national restreint N°00000026/AONR/MPT/CIPM/2021 du 17 aout 2021 lance en procédure d’urgence pour le recrutement d’un cabinet ou bureau d’études en vue du renforcement des capacités du personnel du MINPOSTEL en matière de cyber sécurité » a été lancé le le groupement INTEGC-KIAMA en a été adjudicataire. Ce marché porte sur quatre modules de formation dont la formation CSX PRACTITIONER. Le présent document constitue le rapport de son exécution.

# **Objectifs de la formation**

## Objectif général

Acquérir des connaissances pratiques en cybersécurité.

## Objectifs spécifiques

Les participants à la formation sont désormais capables de :

* Comprendre les concepts sur l’environnement de cybersécurité;
* Comprendre la sécurité opérationnelle (protection) ;
* Reconnaître les menaces ;
* Détecter et évaluer des menaces (Monitoring) ;
* Répondre aux incidents et récupération c’est-à-dire Traitement des incidents, atténuation et restauration;
* Identification et documentation du matériel et du logiciel ;
* Comprendre les concepts Cybercontrôles spécifiques ;
* Savoir-faire une mise à jour des contrôles de cybersécurité.

# **Méthodologie choisie**

Notre méthodologie a consisté en un cours intensif de cinq jours permettant aux participants d’acquérir de bout en bout les différents aspects sur la cyber sécurité.

Durant cette formation, les participants ont appris les différents objectifs et gouvernance de la cybersécurité. Ils ont acquis des notions pratiques sur la cybersécurité.

L’agenda observé est le suivant :

|  |  |  |  |
| --- | --- | --- | --- |
| **Horaire** | **Activités** | **Animateurs** | **Horaire** |
| 08h00-10h00 | Cours | Formateur + Participants | 08h00-10h00 |
| 10h00-10h30 | Pause-café | Formateur + Participants | 10h00-10h30 |
| 10h30-12h30 | Cours | Formateur + Participants | 10h30-12h30 |
| 12h30-13h30 | Pause déjeuner | Formateur + Participants | 12h30-13h30 |
| 13h30-17h00 | Cours | Formateur + Participants | 13h30-17h00 |

# **Déroulement de la formation**

La formation s’est déroulée sur une durée de 5 jours ouvrables et a débuté le lundi 06 décembre 2021 par l’installation des participants et le lancement officiel par les formateurs accompagnés de l’équipe projet de KIAMA SA.

Il a été rappelé les enjeux et les objectifs de la formation puis le matériel de formation a été distribué.

Le programme détaillé de la formation était le suivant :

|  |  |
| --- | --- |
| **Date** | **Modules dispensés** |
| Jour 1 : 06 décembre 2021 | Identifier   * Paiement des frais et configuration de compte * Business Environnent * Environnement de sécurité (ID) |
| `Jour2 : 07 décembre 2021 | Protéger   * Cybercontrôles spécifiques * Contrôles de surveillance * Test de vulnérabilité * Outils et systèmes de sécurité * Points de sauvegarde et de restauration |
| Jour 3 : 08 décembre 2021 | Détecter   * Identification des événements et des incidents * Détection d'événements * Détection et évaluation des menaces |
| Jour 4 : 09 décembre 2021 | Répondre   * Exécution du plan de réponse défini * Notification et confinement des incidents * Recherche et évaluation des logiciels malveillants |
| Jour 5 : 10 décembre 2021 | Atelier   * Identifier * Protéger * Détecter * répondre |

# **Domaines abordés**

Les participants ont été entretenus sur les domaines suivants :

**Domaine 1 : Identifier**

Objectif principal : S’assurer que le candidat à la certification CSX Practitioner est en mesure d’identifier le matériel et le logiciel, les Outils de découverte de réseau, de découvrir les informations sensibles et identifier Processus d'évaluation de la vulnérabilité.

**Domaine 2 : Protéger**

Objectif principal : S’assurer que le candidat à la certification CSX Practitioner est en mesure de comprendre les concepts Cyber contrôles spécifiques, de pouvoir collecter des données d'événement, de savoir installer et configurer le pare-feu, utiliser les normes de procédures de cybersécurité.

**Domaine 3 : Détecter**

Objectif principal : S’assurer que le candidat à la certification CSX Practitioner est en mesure d’analyser le trafic réseau à l'aide de moniteurs, de détecter les activités malveillantes Antivirus, d’évaluer les informations disponibles sur l'événement.

**Domaine 4 : Répondre**

Objectif principal : S’assurer que le candidat à la certification CSX Practitioner est en mesure d’exécuter du plan de réponse défini, de pouvoir faire un isolement du réseau, de désactiver les comptes d'utilisateurs, d’implémenter des modifications de système unique dans le pare-feu.

**Domaine 5 : Récupérer**

Objectif principal : S’assurer que le candidat à la certification CSX Practitioner est en mesure de comprendre les concepts clés de la sauvegarde et de la restauration des données, de planifier une restauration du système informatique et d’implémenter des correctifs et des mises à jour.

# **Conclusion**

Le cabinet KIAMA SA, bénéficiaire du marché de renforcement des capacités du personnel du MINPOSTEL en matière de cyber sécurité a, dans cette étape réalisé le second module portant sur la formation à la certification CSX Practitioner. Il était question dans cette phase du marché, d’assurer la formation de six (06) personnels du MINPOSTEL sur la cybersécurité. La formation s’est déroulée comme prévu, les participants ont tous répondu présents. Ils ont bénéficié des attestations officielles de fin de formation et de leur inscription pour le passage de l’examen de certification selon leur disponibilité.

Le suivi d’après formation est effectif et se déroule dans le groupe whatsapp créé à cet effet et dont le lien est <https://chat.whatsapp.com/GRpm1xXf1gAGkeICtQ21Tz>.

Dans ce groupe, les apprenants remontent les difficultés éventuelles auxquelles ils font face et son coachés en prélude à leur examen.

Le personnel formé termine cette formation, enrichi de l’expérience sur la notion de cybersécurité. Aussi le formateur s’est assuré que ces derniers prendront le soin de bien appliquer les notions apprises dans le but d’aider le MINPOSTEL en général et la DSR en particulier à mieux réaliser ses missions.

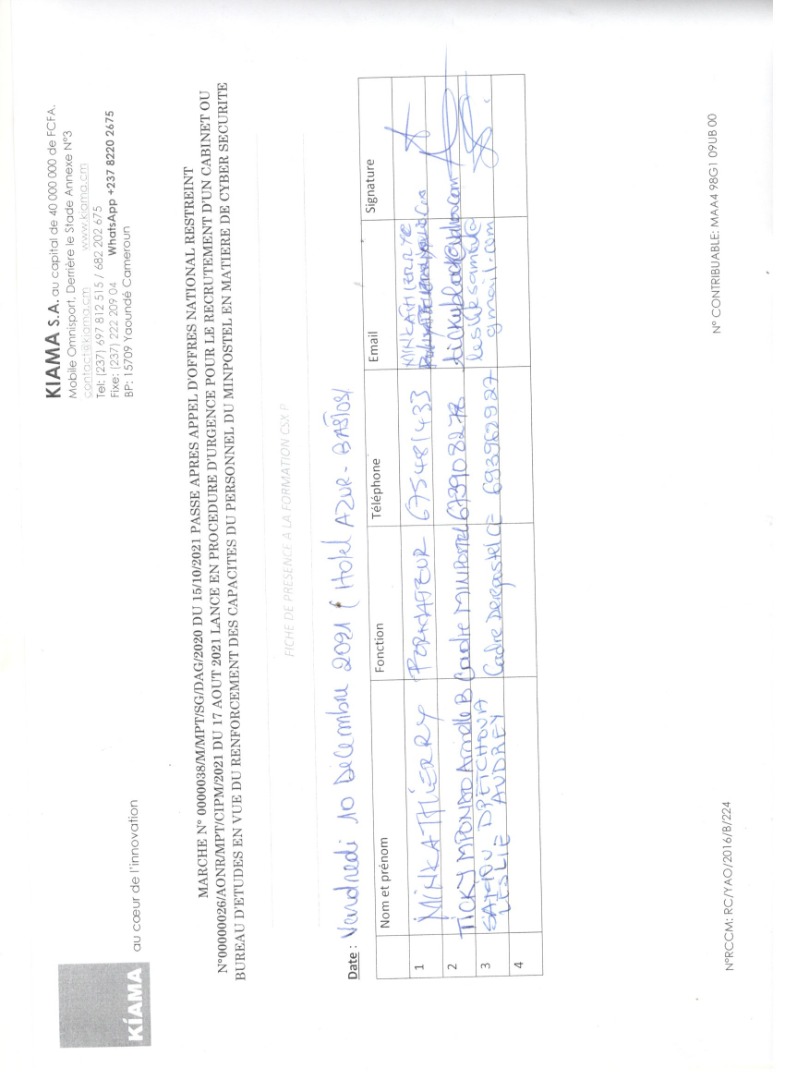
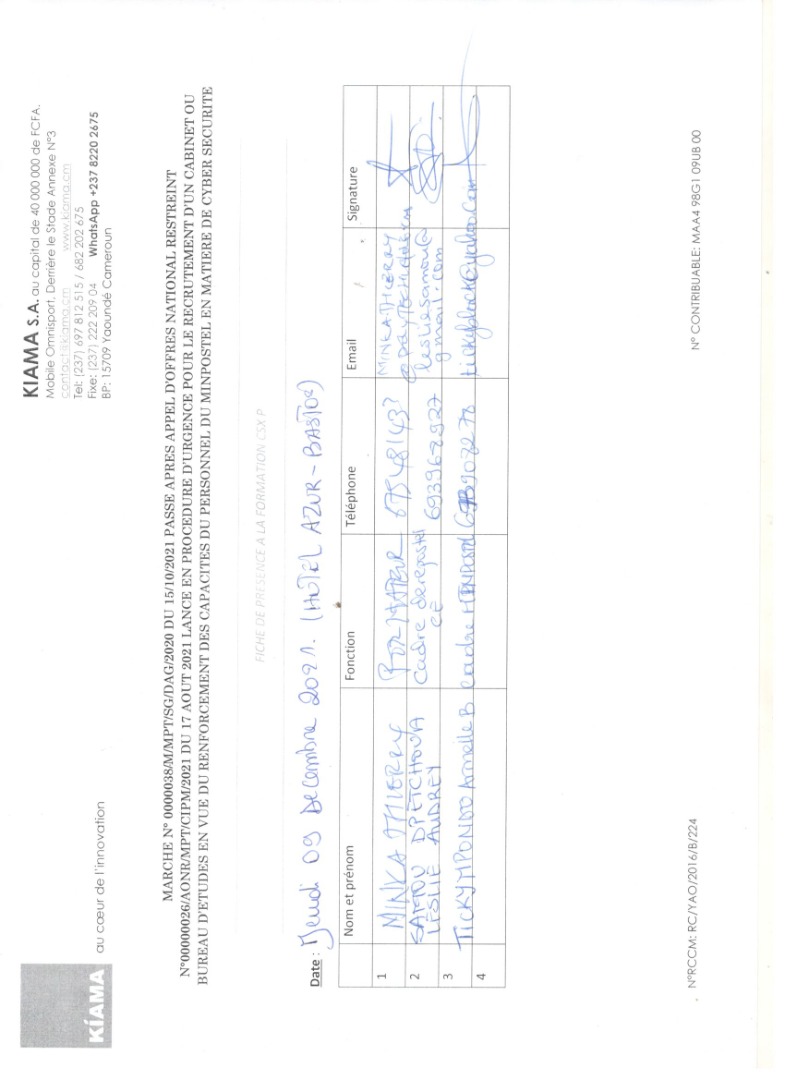
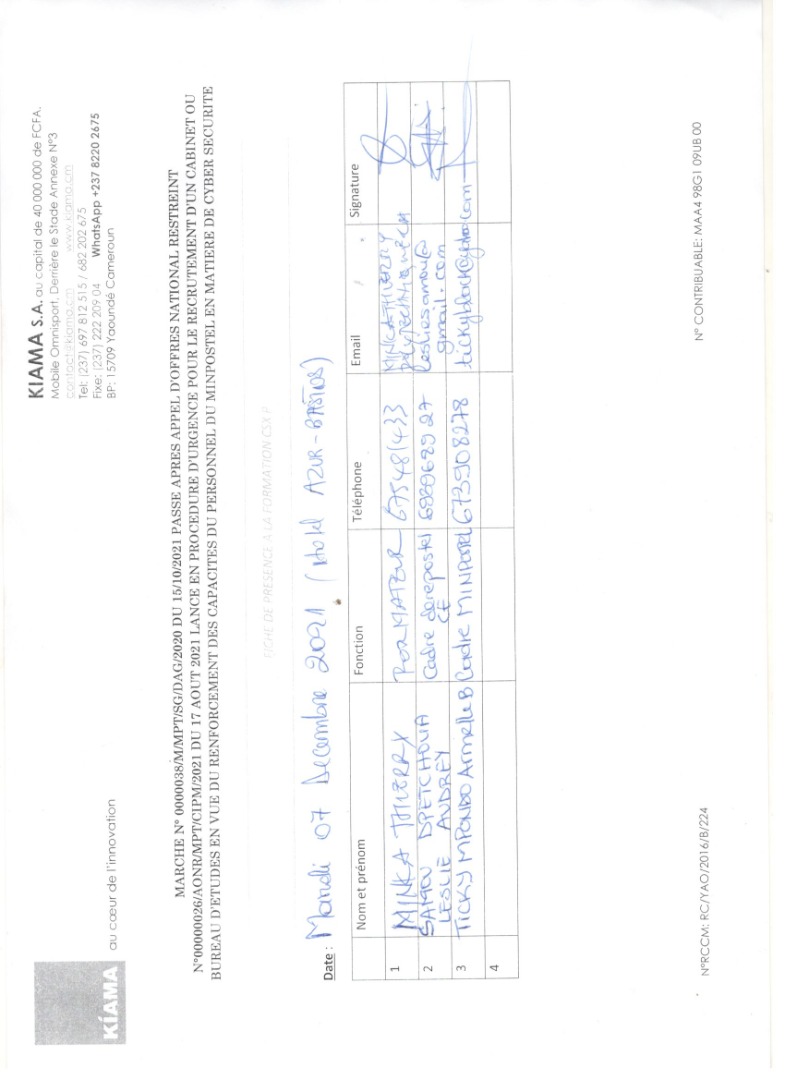
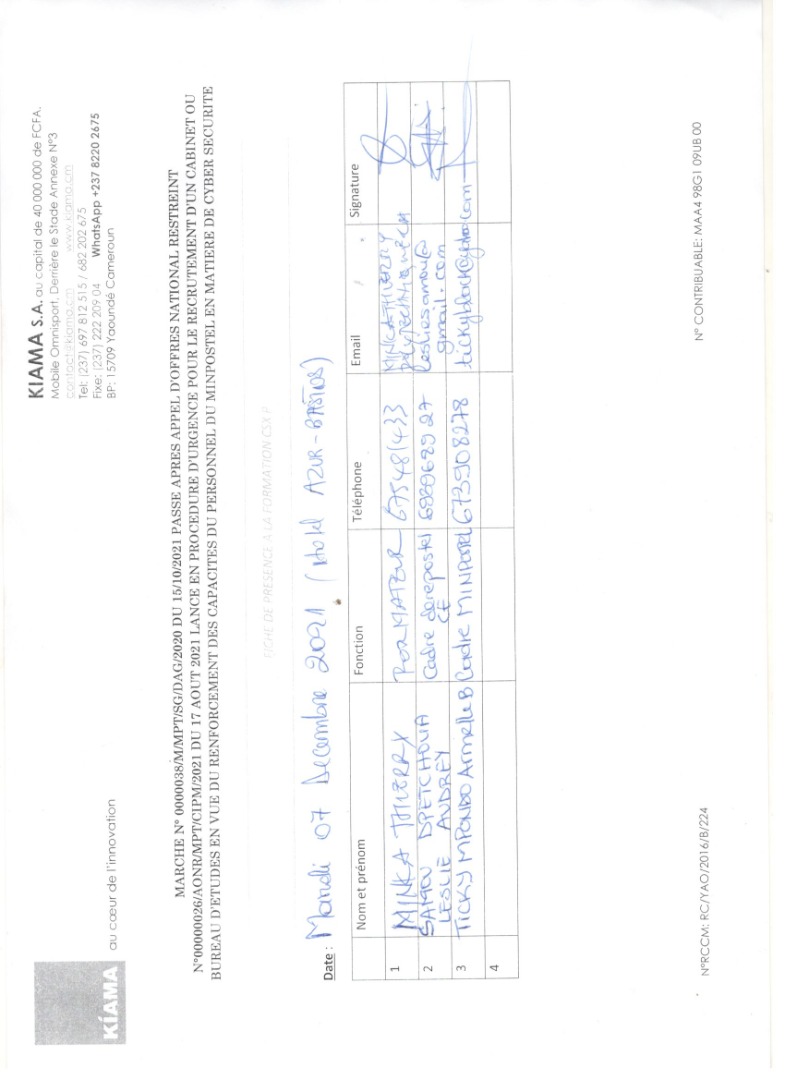
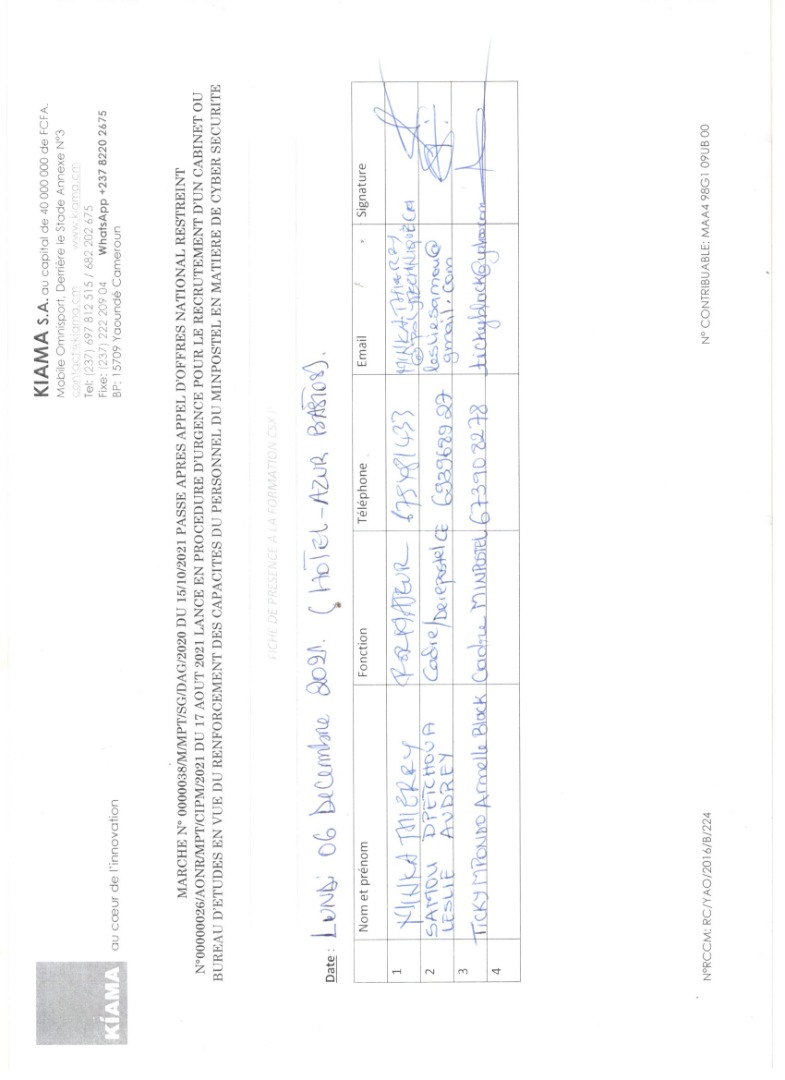
# ANNEXES

# A1/ ATTESTATIONS DE PARTICIPATION





# A2/ LISTES DE PRESENCE



# A3/ PHOTO DE FAMILLE

