|  |  |  |
| --- | --- | --- |
| **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 FUNDAMENTALS**

**Décembre 2021**





**RAPPORT DE LA FORMATION SUR CSX FUNDAMENTALS**





LE PRESENT DOCUMENT EST LE RAPPORT DE LA FORMATION SUR LE MODULE CSX FUNDAMENTALS 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](#_Toc90284095)

[**2.** **Introduction et contexte** 7](#_Toc90284096)

[**3.** **Objectifs de la formation** 9](#_Toc90284097)

[3.1. Objectif général 9](#_Toc90284098)

[3.2. Objectifs spécifiques 9](#_Toc90284099)

[**4.** **Méthodologie choisie** 10](#_Toc90284100)

[**5.** **Déroulement de la formation** 11](#_Toc90284101)

[**6.** **Domaines abordés** 13](#_Toc90284102)

[**7.** **Conclusion** 14](#_Toc90284103)

[ANNEXES 15](#_Toc90284104)

[A1/ ATTESTATIONS DE PARTICIPATION 16](#_Toc90284105)

[A2/ LISTES DE PRESENCE 19](#_Toc90284106)

[A3/ PHOTOS DE FAMILLE 25](#_Toc90284107)

# **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 et le groupement INTEGC-KIAMA en a été adjudicataire. Ce marché porte sur quatre modules de formation parmi lesquels la formation CSX Fundamentals. Le présent document constitue le rapport de son exécution.

# **Objectifs de la formation**

## Objectif général

Acquérir des connaissances de bases en cybersécurité.

## Objectifs spécifiques

Les participants à la formation sont désormais capables de :

* Comprendre les concepts et définitions de base de la cybersécurité ;
* Comprendre les principes de base de la gestion et de l'évaluation des risques liés aux menaces de cybersécurité ;
* Reconnaître les méthodologies et les techniques de détection des intrusions sur l'hôte et le réseau via les technologies de détection des intrusions
* Distinguer les menaces et les vulnérabilités de la sécurité des systèmes et des applications ;
* Reconnaître les principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
* Reconnaître les technologies de l'information et les informations nouvelles et émergentes
* Définir les concepts d'architecture de sécurité réseau

# **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 pu discerner la différence entre la sécurité de l’information et la cybersécurité.

L’agenda observé était le suivant :

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

# **Déroulement de la formation**

La formation s’est déroulée sur une durée de 5 jours ouvrables et a débuté le lundi 22 novembre 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 : 22 novembre 2021 | Introduction et aperçu de la cybersécurité   * Introduction à la cybersécurité * Différence entre sécurité de l'information et cybersécurité * Objectifs de cybersécurité * Rôles de la cybersécurité * Domaines de la cybersécurité |
| `Jour 2 : 23 novembre 2021 | Concepts de cybersécurité   * Risques * Types et vecteurs d'attaque courants * Politiques et procédures * Contrôles de la cybersécurité |
| Jour 3 : 24 novembre 2021 | Principes de l'architecture de sécurité   * Le modèle OSI * Défense en profondeur * Pare-feu * Isolation et segmentation * Surveillance, détection et journalisation * Principes fondamentaux du chiffrement * Techniques de cryptage * Applications du cryptage |
| Jour 4 : 25 novembre 2021 | Sécurité des réseaux, des systèmes, des applications et des données   * Contrôles des processus - Évaluations des risques * Contrôles des processus - Gestion des vulnérabilités * Contrôles des processus - Tests de pénétration * Sécurité des réseaux * Sécurité des systèmes d'exploitation * Sécurité des applications * Sécurité des données |
| Jour 5 : 26 novembre 2021 | Préparation pratique à l’examen de certification |

# **Domaines abordés**

Les participants ont été entretenus sur les domaines suivants :

**Domaine 1 : Concepts de cybersécurité**

Objectif principal : S’assurer que le candidat à la certification CSX Fundamentals est en mesure de comprendre la gestion de base des risques, la notion de Vecteurs d'attaque et agents de menace courants, les Modèles et types d’attaques, les Types de politiques et de procédures de sécurité et les Processus de contrôle de la cybersécurité.

**Domaine 2 : Principes de l'architecture de sécurité**

Objectif principal : S’assurer que le candidat à la certification CSX Fundamentals est en mesure de comprendre, interpréter et illustrer les architectures et cadres de sécurité courants, les concepts de sécurité du périmètre, les pare-feu et le cryptage.

**Domaine 3 : Sécurité des réseaux, des systèmes, des applications et des données**

Objectif principal : S’assurer que le candidat à la certification CSX Fundamentals est en mesure de comprendre, interpréter et appliquer les principes de l'architecture de sécurité, les concepts de sécurité du périmètre, les pare-feu et le cryptage.

**Domaine 4 : Réponse aux incidents**

Objectif principal : S’assurer que le candidat à la certification CSX Fundamentals est en mesure de pouvoir faire la distinction essentielle entre un événement et un incident. Plus important encore, il sera capable de décrire les étapes nécessaires à la réponse à un incident de cybersécurité.

**Domaine 5 : Implications en matière de sécurité et adoption de technologies en constante évolution**

Objectif principal : S’assurer que le candidat à la certification CSX Fundamentals est en mesure de décrire le paysage actuel des menaces, y compris une discussion des vulnérabilités associées aux technologies émergentes

# **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 Fundamentals. Il était question dans cette phase du marché, d’assurer la formation de six (06) personnels du MINPOSTEL sur la cybersécurité fondamentale. 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.

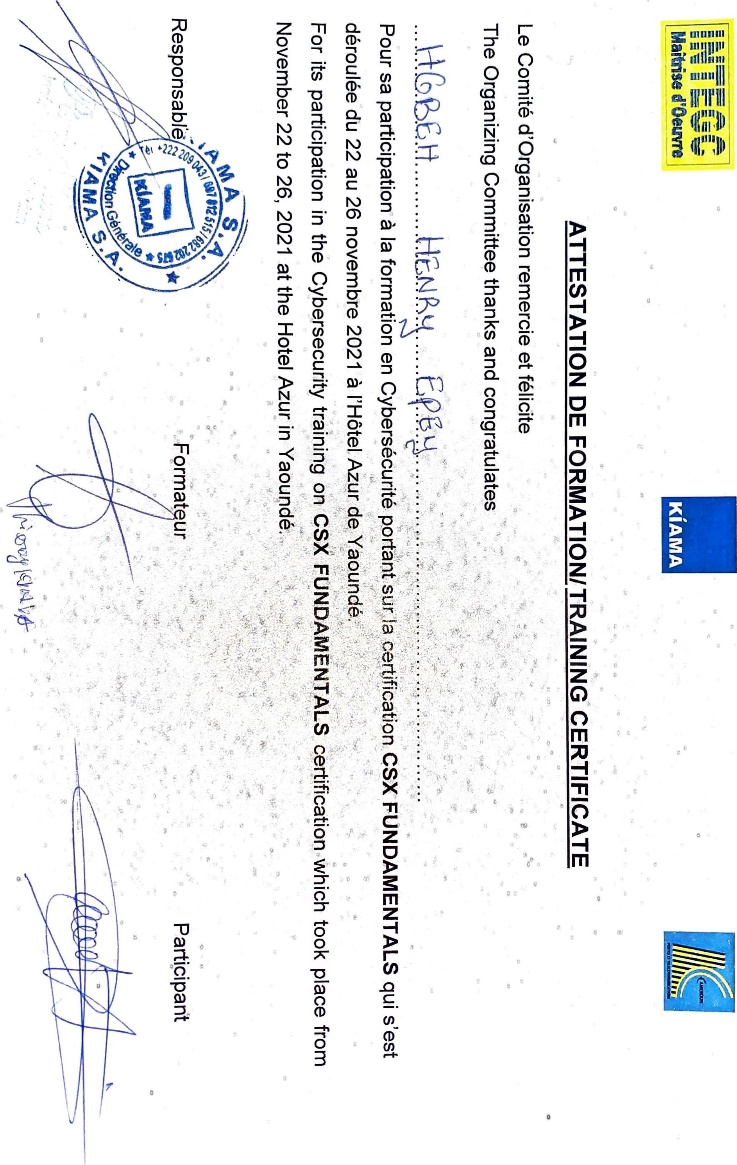
Le suivi d’après formation est effectif et se déroule dans le groupe whatsapp créé à cet effet et dont le lien est <https://chat.whatsapp.com/FnRWLaDJzlSK0gBXZKwxVN>.

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

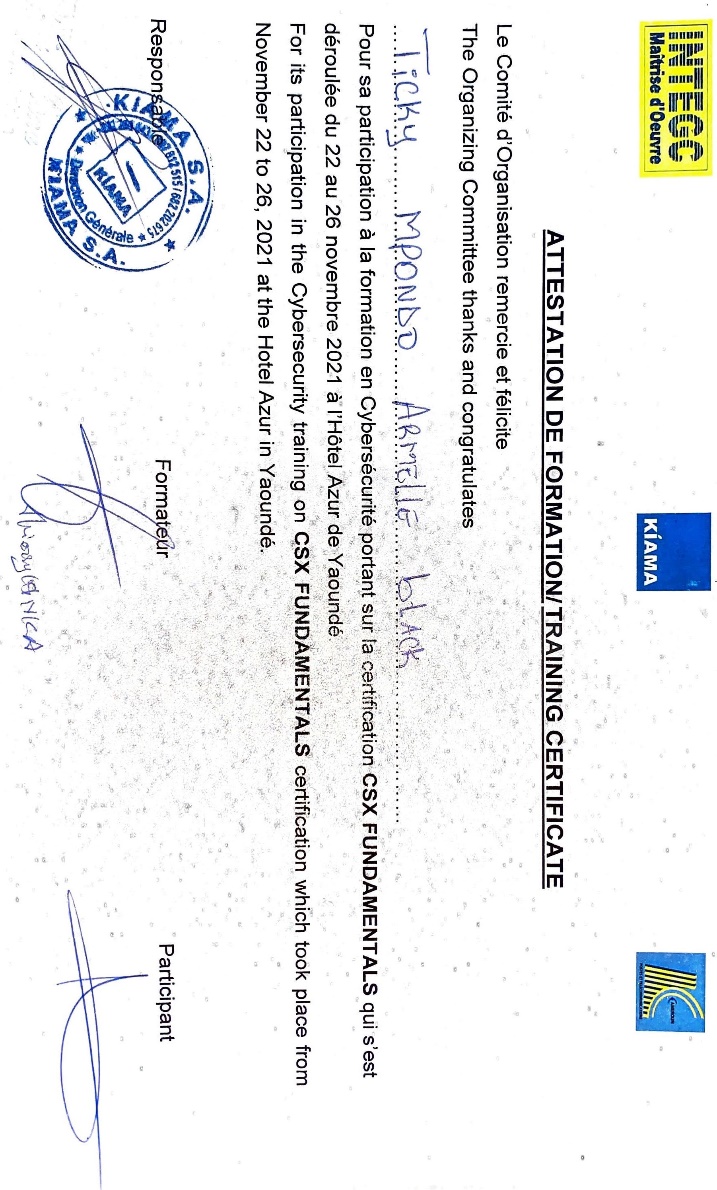
Le personnel formé termine cette formation, enrichi de l’expérience sur la notion de cybersécurité. Aussi le formateur s’est assuré que ces derniers prendront le soin de bien appliquer les notions apprises dans le but d’aider le MINPOSTEL en général et la DSR en particulier à mieux réaliser ses missions.

# ANNEXES

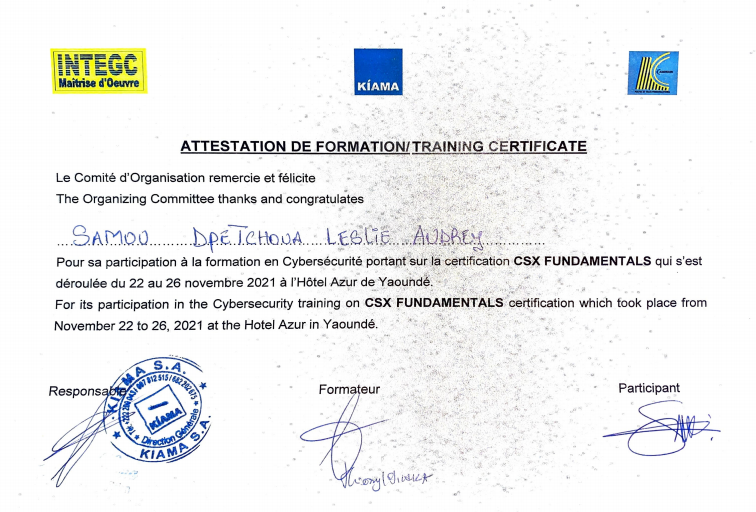
# A1/ ATTESTATIONS DE PARTICIPATION





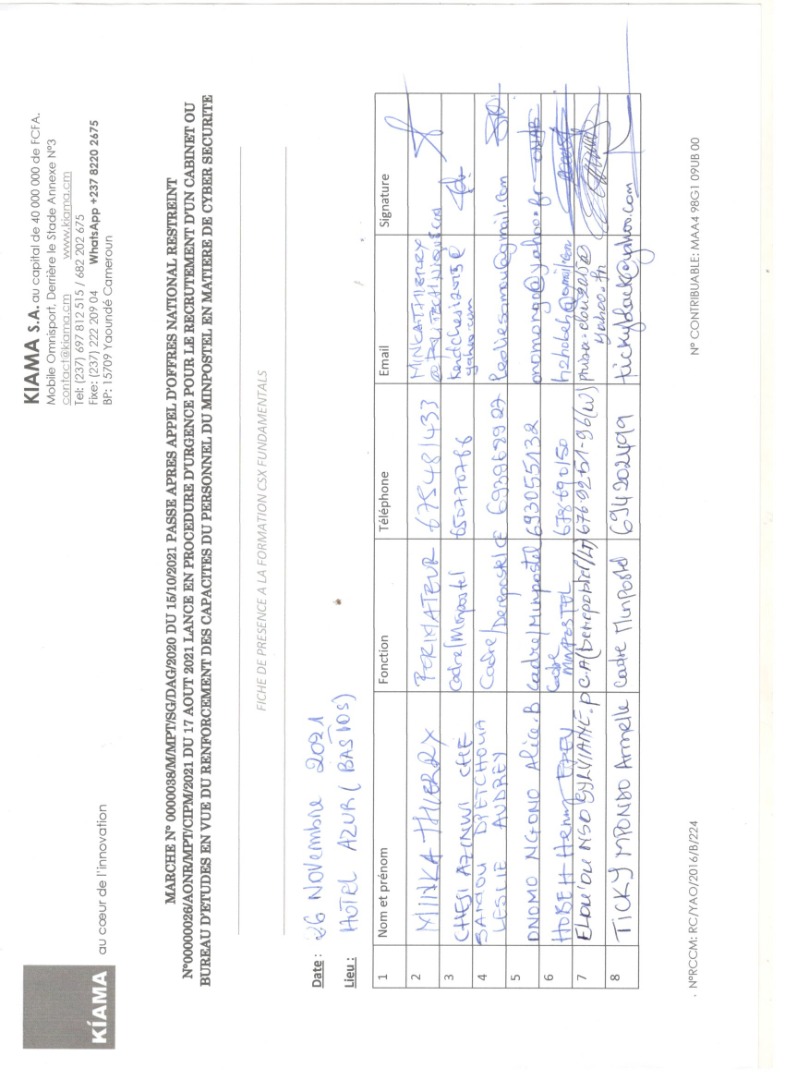
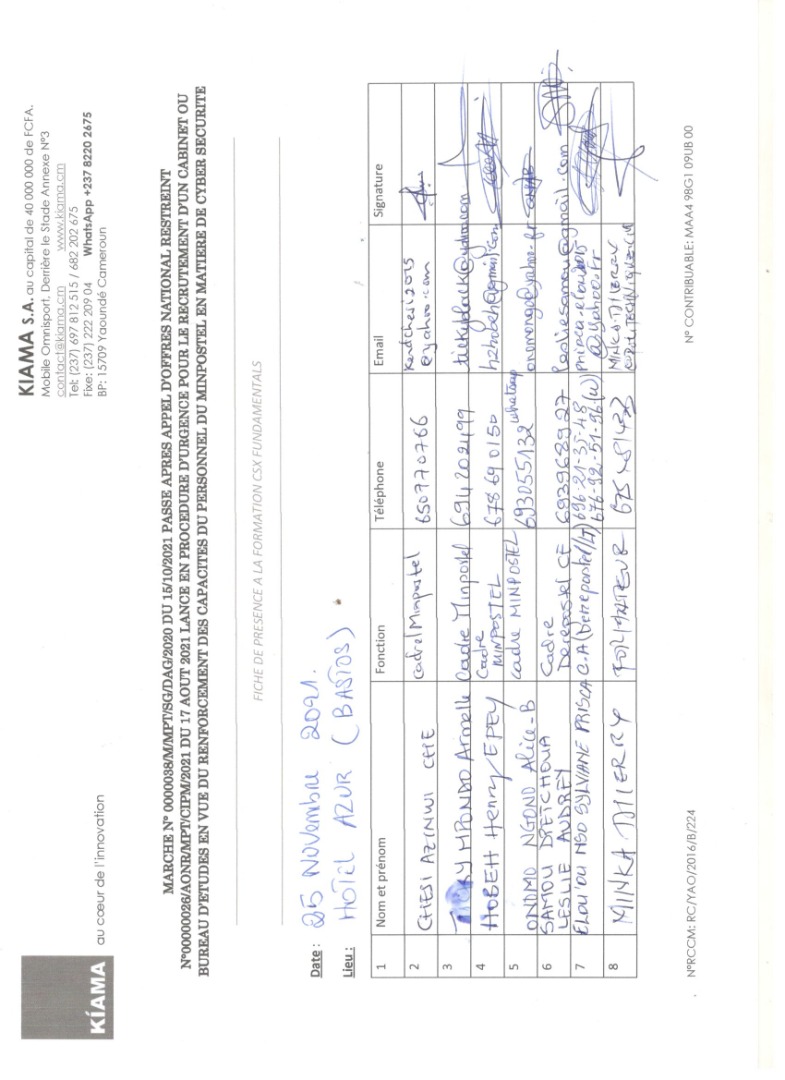
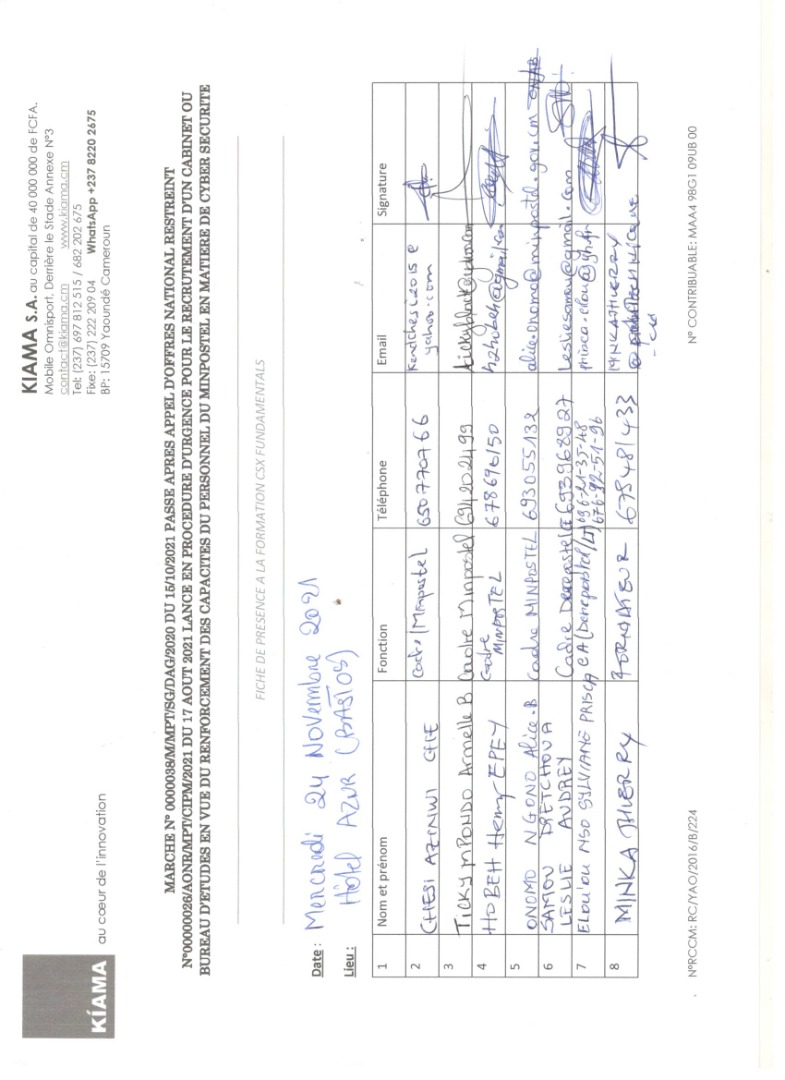
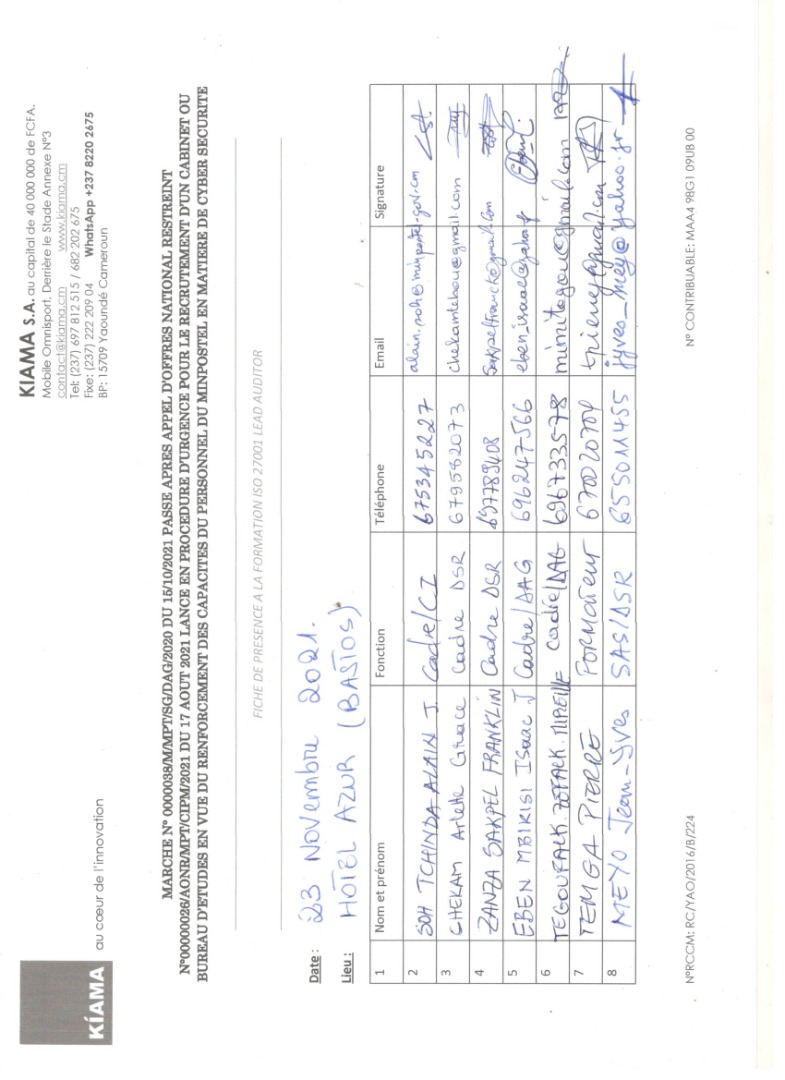
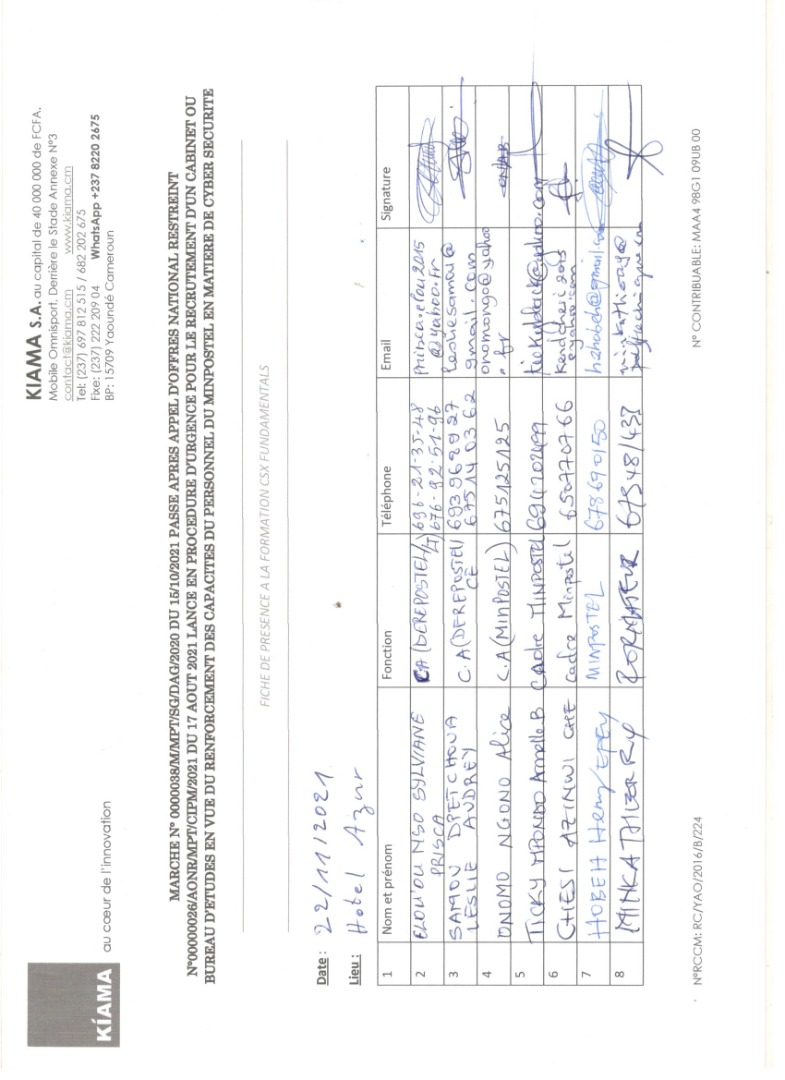








# A2/ LISTES DE PRESENCE



# A3/ PHOTOS DE FAMILLE

