

Nature du document	TDRs pour le recrutement d'un consultant national
Intitulé de la mission	Animation de l'atelier de formation sur la sécurité numérique (cybersécurité)
Financement	Subvention GC7 du Fonds mondial, Récipiendaire principal : PNUD Burundi

1. Contexte et justification

Les activités de l'ANSS-Santé PLUS reposent chaque jour un peu plus sur des outils numériques : ordinateurs, smartphones, courriels, messageries et plateformes de données. Le personnel y traite des données personnelles et de santé de bénéficiaires, ainsi que des données de projet.

Les menaces informatiques se multiplient (hameçonnage, rançongiciels, vol de données, compromission de mots de passe) et l'erreur humaine reste souvent la première faille exploitée. Une fuite de données de bénéficiaires pourrait porter tort aux personnes concernées, et un rançongiciel bloquerait les postes de travail et interromprait les activités.

Pour instaurer une culture interne de vigilance, l'ANSS prévoit un atelier pratique de deux jours en sécurité numérique pour 147 participants (personnel de l'ANSS-Santé PLUS et huit agents d'organisations partenaire) répartis en six sessions. L'ANSS-Santé PLUS désire recruter un consultant national pour concevoir et animer cet atelier.

2. Objectifs de la mission

Objectif général. Renforcer les capacités techniques et les réflexes de sécurité de base des collaborateurs face aux cybermenaces quotidiennes.

Objectifs spécifiques.

- Adapter le programme aux outils et aux usages de l'ANSS-Santé PLUS et de ses partenaires (postes de travail, smartphones, messageries, télétravail).
- Animer les six sessions : exposés, études de cas réels, démonstrations pratiques, questions et réponses.
- Vérifier à la fin de chaque session que les participants maîtrisent les bonnes pratiques d'hygiène numérique.
- Remettre une fiche réflexe sur les règles d'hygiène numérique et sur la procédure d'alerte en cas d'incident.

3. Tâches du consultant

3.1 Préparation

- Étudier les TDRs de l'activité et échanger avec le responsable IT sur les outils utilisés, les pratiques courantes et les incidents déjà rencontrés.
- Rédiger la note méthodologique et le programme détaillé de chaque session de deux jours.
- Produire les supports, les études de cas, les démonstrations, le quiz d'évaluation et la fiche réflexe.

Le programme comprend quatre modules. Le premier présente les notions fondamentales (confidentialité, intégrité, disponibilité), le panorama des cybermenaces actuelles et le profil des attaquants. Le deuxième traite de l'hygiène informatique de l'utilisateur : gestion des mots de passe, authentification multifacteur, sécurité des postes de travail, des smartphones et des réseaux Wi-Fi, au bureau comme en télétravail. Le troisième porte sur

les pièges courants : reconnaître l'hameçonnage et les faux courriels, comprendre la manipulation psychologique et l'ingénierie sociale. Le quatrième décrit la conduite à tenir en cas d'incident : procédure d'alerte interne et premiers réflexes d'isolement d'une machine compromise.

3.2 Animation des sessions

Le consultant anime six sessions de deux jours. Deux ont lieu à Bujumbura pour les participants issus de la Direction exécutive, du centre médico-social Turiho et des organisations partenaires. Quatre ont lieu aux chefs-lieux des antennes de Rumonge, Makamba, Gitega et Kirundo. L'itinéraire prévu au budget est Bujumbura, Rumonge, Makamba, Gitega, Kirundo, puis retour à Bujumbura.

La formation s'adresse à des utilisateurs ordinateurs, sans formation informatique : le consultant emploie un langage non technique.

3.3 Évaluation et rapportage

- Vérifier les acquis à la fin de chaque session par un court quiz.
- Relever les pratiques à risque évoquées pendant les échanges et les démonstrations, pour les transmettre au coordonnateur IT.
- Présenter un rapport final au point focal.

4. Livrables

N°	Livrable	Échéance
1	Note méthodologique, programme détaillé de deux jours et chronogramme des six sessions	Trois jours au moins avant la première session
2	Supports de formation, études de cas, démonstrations, quiz d'évaluation et fiche réflexe (règles d'hygiène numérique et procédure d'alerte en cas d'incident), en versions électroniques	Trois jours au moins avant la première session, après validation par le point focal
3	Rapport final : déroulement de chaque session, effectifs par site, résultats du quiz, pratiques à risque observées, recommandations pour le coordonnateur IT. Annexes : listes de présence signées et supports utilisés	Sept jours après la dernière session

5. Durée et lieu d'exécution

La préparation des modules de formation est planifiée sur 2 jours, la formation représente douze jours de facilitation (six sessions de deux jours), à réaliser après la signature du contrat et avant la fin du mois d'octobre 2026. Les dates exactes de chaque session sont arrêtées avec le point focal dès le démarrage. Les sessions se tiennent à Bujumbura et aux chefs-lieux des quatre antennes. La préparation du rapport final de la consultance est planifiée sur 2 jours.

6. Profil requis

- **Nationalité** : burundaise.
- **Formation** : diplôme universitaire en informatique, réseaux et télécommunications, sécurité des systèmes d'information ou domaine voisin. Une certification en cybersécurité est un atout.
- **Expérience** : cinq ans au moins en sécurité informatique ou en administration de systèmes ; trois actions au moins de formation ou de sensibilisation de personnel non spécialiste à la cybersécurité.
- **Connaissances** : hameçonnage, maliciels, rançongiciels, ingénierie sociale ; gestion des mots de passe et authentification multifacteur ; sécurisation des smartphones et des réseaux Wi-Fi ; réaction de base à un incident ; pédagogie active auprès d'adultes.
- **Langues** : français et Kirundi courant, à l'oral comme à l'écrit.
- **Atouts** : expérience auprès d'ONG, de structures de santé ou de projets financés par le Fonds mondial et mis en œuvre avec le PNUD ; connaissance de la protection des données personnelles et de santé.
- **Disponibilité** : pour douze jours de formation, dont huit hors de Bujumbura, sur la période indiquée.

7. Encadrement et conditions de la mission

Le consultant travaille sous la supervision du point focal de l'activité. La coordination du projet GC7 valide les livrables. Il s'engage à garder confidentielles les informations recueillies sur les pratiques et les incidents de sécurité de l'ANSS-Santé PLUS.

L'ANSS-Santé PLUS assure le transport du consultant dans un véhicule de l'association avec chauffeur, ses per diem pendant la tournée dans les antennes, le kit du formateur (flip chart et marqueurs) ainsi que les pauses et déjeuners des participants. Le consultant apporte son ordinateur portable.

Les honoraires couvrent aussi la préparation des supports, la fiche réflexe et le rapport final. Les impôts et retenues applicables sont traités conformément à la réglementation burundaise et aux procédures de l'ANSS-Santé PLUS.

Le paiement se fait après la validation du rapport final.

8. Candidature et sélection

L'évaluation des offres se fera en deux étapes :

1. Evaluation des offres techniques, portant notamment sur les qualifications et l'expérience du consultant, les références de missions similaires ainsi que la qualité de la note méthodologique proposée.
2. Evaluation des offres financières sera effectuée après l'analyse des offres techniques.
 - a) **L'offre technique** : elle comprendra une lettre de motivation, un CV détaillé, les copies des diplômes et attestations, deux références de missions comparables et une note méthodologique de deux pages au plus décrivant l'organisation proposée pour les deux jours de formation.
 - b) **L'offre financière** : elle comprendra une proposition financière détaillée présentant les honoraires du consultant liés à la réalisation de la mission.

L'offre technique et l'offre financière devront être présentées sous plis fermés et séparés, chacun portant clairement la mention correspondante (« Offre technique » ou « Offre financière »). Les deux plis séparés seront ensuite placés dans une seule enveloppe, fermée qui sera déposée au bureau de la Direction Exécutive de l'ANSS-Santé PLUS (6, avenue Muhabo, Kigobe, Bujumbura) au plus tard le 15/10/2026.

L'évaluation technique porte sur les critères techniques suivants, conformément aux procédures de l'ANSS-Santé PLUS et aux exigences du Récipiendaire Principal :

Critère	Points
Diplôme en informatique, réseaux ou sécurité des systèmes d'information ; (une certification en cybersécurité est un atout)	15
Expérience en sécurité informatique ou administration de systèmes	25
Expérience de formation ou de sensibilisation de personnel non spécialiste en cybersécurité	25
Expérience auprès d'ONG, de structures de santé ou de projets financés par des bailleurs internationaux	10
Note méthodologique	25
Total	100

Les critères « qualité technique » et « coût » seront notés chacun sur un maximum de 100 points dans un premier temps puis ramené à la pondération de 80% pour le critère « qualité technique » contre 20% pour le critère « coût ». Les notes obtenues pour chaque critère par prestataire, seront ensuite additionnées et le prestataire qui aura obtenu le score le plus élevé sera retenu et invité à négocier le contrat, à condition qu'il/elle ait obtenu le score minimal de qualification technique requis de 70%.

Fait à Bujumbura, le 28/09/2026

La Directrice Exécutive de l'ANSS Santé PLUS

Madame KABUGUBUGU Martine

