UCLG AFRICA
United Cities and Local Governments of Africa
Cités et Gouvernements Locaux Unis d'Afrique
CGLU AFRIQUE

TERMES DE RÉFÉRENCE

Cadre Systèmes d'Information (SI)

1. Contexte

En vue du renforcement de ses fonctions de gestion et de la consolidation de son fonctionnement institutionnel, CGLU Afrique préconise, dans le cadre de sa nouvelle gouvernance, de recruter un Cadre Systèmes d'information (SI) renforcer ses capacités internes de gestion, de sécurisation et de développement de ses systèmes d'information.

Cette démarche repose sur une meilleure maîtrise des infrastructures et services numériques, la sécurisation des accès et des données, la disponibilité des outils de travail et l'organisation d'un dispositif de gestion et de support adapté aux besoins de l'organisation.

Elle vise également à garantir l'autonomie de CGLU Afrique dans l'administration de ses actifs numériques, la continuité de ses services et la maîtrise des prestations informatiques externes.

Placé sous la responsabilité hiérarchique du Secrétaire Général, le titulaire du poste devra remplir les conditions suivantes :

2. Mission générale

Le cadre SI assure la gestion, le pilotage opérationnel, la maintenance et la sécurisation du système d'information de CGLU Afrique.

Il garantit la disponibilité des infrastructures, applications et services numériques, la protection des données, la gestion maîtrisée des accès ainsi que la continuité des activités de l'organisation.

Il assure directement les activités d'administration et de support relevant de ses compétences et coordonne, lorsque nécessaire, l'intervention de prestataires spécialisés.

Il accompagne l'évolution des outils et solutions numériques en fonction des besoins des utilisateurs et des priorités de CGLU Afrique.

Il veille à la documentation et à la traçabilité des configurations, des accès, des interventions et des actifs numériques, afin de garantir la maîtrise durable du système d'information par l'organisation.

3. Gouvernance et pilotage du système d'information

- Établir et tenir à jour la cartographie du système d'information, des applications, des infrastructures, des services numériques et de leurs principales interdépendances.

- Identifier les besoins d'évolution du système d'information en coordination avec les responsables des fonctions concernées.
- Élaborer et actualiser une feuille de route SI intégrant les besoins fonctionnels, les priorités techniques, les risques et les investissements nécessaires.
- Préparer les propositions budgétaires relatives aux équipements, logiciels, licences, hébergements et prestations informatiques.
- Assurer le suivi des dépenses et des engagements informatiques en coordination avec la fonction administrative et financière.
- Définir et documenter les procédures d'exploitation, de maintenance, de sécurité et de gestion des changements.
- Veiller à la cohérence des solutions numériques retenues et à leur adéquation avec les besoins de CGLU Afrique.
- Préparer les analyses et recommandations nécessaires aux décisions et arbitrages de la direction.

4. Gestion des infrastructures et des actifs numériques

- Assurer l'inventaire et le suivi des équipements informatiques, serveurs, postes de travail, équipements réseau et autres infrastructures numériques.
- Administrer et superviser les services d'hébergement, les environnements cloud, les réseaux et les outils de communication électronique.
- Garantir la disponibilité et le bon fonctionnement des services essentiels, notamment la messagerie professionnelle, le site internet, les outils collaboratifs et les espaces de stockage documentaire.
- Tenir à jour le registre des noms de domaine, hébergements, licences, abonnements, contrats et services numériques utilisés par CGLU Afrique.
- Assurer l'installation, la configuration, la maintenance et le renouvellement des équipements et logiciels informatiques.
- Documenter les configurations techniques, les comptes d'administration, les modalités d'accès et les dispositifs de récupération des services.
- Veiller à ce que les actifs numériques, comptes stratégiques et moyens de récupération soient administrés dans un cadre institutionnel maîtrisé par CGLU Afrique, sans dépendance exclusive à des comptes personnels ou à des prestataires externes.
- Organiser et suivre les interventions de maintenance préventive et corrective.

5. Gestion des accès et cybersécurité

- Définir et mettre en œuvre les mesures de sécurité adaptées aux infrastructures, applications et données de CGLU Afrique.
- Organiser la gestion des identités et des habilitations en fonction des responsabilités des utilisateurs et des autorisations formellement accordées.
- Assurer la création, la modification, la suspension et la suppression des accès, notamment lors des mouvements du personnel et des changements de responsabilités.
- Mettre en œuvre les dispositifs appropriés de sécurisation des accès, notamment l'authentification multifacteur pour les comptes sensibles et les accès d'administration.
- Veiller à la protection des comptes privilégiés et à la sécurisation des moyens de récupération des accès.
- Assurer la mise à jour des systèmes, le suivi des vulnérabilités et la mise en œuvre des mesures de protection contre les risques informatiques.
- Organiser la surveillance des services critiques, la détection des anomalies et le traitement des incidents de sécurité.
- Documenter les incidents, les mesures correctives et les actions nécessaires à la prévention de leur réapparition.
- Sensibiliser les utilisateurs aux bonnes pratiques de sécurité informatique et de protection des informations.

6. Sauvegardes, continuité et reprise des activités

- Définir et mettre en œuvre une politique de sauvegarde des données, applications et configurations essentielles au fonctionnement de CGLU Afrique.
- Organiser les sauvegardes selon des fréquences et modalités adaptées à la criticité des informations et des services.
- Assurer le suivi de la bonne exécution des sauvegardes et le traitement des anomalies constatées.
- Réaliser périodiquement des tests de restauration afin de vérifier la disponibilité et l'exploitabilité des données sauvegardées.
- Élaborer et maintenir les procédures de continuité et de reprise des services numériques en cas de panne, d'incident de sécurité ou d'indisponibilité majeure.
- Définir les priorités et objectifs de rétablissement des services en fonction de leur importance pour les activités de l'organisation.
- Coordonner la réponse aux incidents majeurs, les interventions techniques et l'information des responsables concernés.

- Documenter les tests, incidents et opérations de reprise, et assurer le suivi des actions d'amélioration.

7. Applications, données et gestion documentaire

- Assurer l'administration technique, la maintenance et le bon fonctionnement des applications et outils métiers utilisés par CGLU Afrique.
- Garantir la disponibilité et la maintenance technique des solutions comptables et de gestion, notamment SAGE, en coordination avec les responsables fonctionnels concernés.
- Accompagner les utilisateurs dans l'exploitation des applications, la résolution des difficultés techniques et l'évolution des outils.
- Organiser la gestion des espaces documentaires numériques, des droits d'accès et des dispositifs de partage sécurisé de l'information.
- Veiller à la disponibilité, à l'intégrité et à la traçabilité des données et documents électroniques.
- Mettre en œuvre les règles de conservation, d'archivage et de suppression des données définies avec les responsables métiers et la fonction juridique.
- Assurer la sécurisation des échanges numériques avec les partenaires, programmes et entités associés à CGLU Afrique.
- Veiller à la séparation appropriée des accès et des données lorsque plusieurs programmes ou entités utilisent des infrastructures ou applications communes.
- Contribuer aux projets d'évolution, d'intégration ou de remplacement des applications, en garantissant la conservation et la récupération des données.

8. Support aux utilisateurs et gestion des prestataires

- Assurer l'assistance technique aux utilisateurs des équipements, applications et services numériques.
- Organiser le traitement et le suivi des demandes d'assistance et des incidents informatiques.
- Définir et suivre les délais d'intervention et de résolution selon la criticité des incidents.
- Diagnostiquer et résoudre les dysfonctionnements techniques relevant de son périmètre de compétences.
- Identifier les besoins nécessitant le recours à des prestataires spécialisés et préparer les éléments techniques correspondants.
- Coordonner les interventions des fournisseurs, éditeurs, hébergeurs et autres prestataires techniques.

- Assurer le suivi des contrats, licences, abonnements, engagements de service et échéances techniques.
- Vérifier la qualité des prestations réalisées et signaler les insuffisances ou manquements constatés.
- Documenter les interventions techniques, les changements de configuration et les opérations de maintenance significatives.
- Organiser le transfert de connaissances et maintenir une documentation technique permettant la continuité de l'exploitation.
- Veiller à la réversibilité des prestations externalisées, notamment par la disponibilité des accès institutionnels, des configurations, des données et des procédures nécessaires à leur reprise.

9. Reporting, contrôles et audits SI

- Produire un tableau de bord périodique présentant la disponibilité des services, les incidents, les interventions, les risques et les actions en cours.
- Tenir à jour les inventaires techniques, les registres des accès sensibles, des licences, des sauvegardes et des contrats informatiques.
- Identifier les risques affectant la sécurité, la disponibilité ou la continuité des services numériques et proposer les mesures correctives appropriées.
- Préparer les analyses et justificatifs techniques nécessaires aux audits et contrôles portant sur le système d'information.
- Contribuer à la mise en œuvre et au suivi des recommandations d'audit relevant de son périmètre.
- Assurer la traçabilité des interventions significatives et préserver les informations techniques nécessaires aux vérifications et investigations autorisées.
- Produire les éléments nécessaires aux décisions concernant les investissements, les évolutions techniques et le renouvellement des prestations.

10. Profil et compétences recherchés

- Bac+5 en informatique, systèmes d'information, cybersécurité, télécommunications ou formation équivalente.
- Minimum huit années d'expérience pertinente dans la gestion, l'exploitation et la sécurisation de systèmes d'information, dont une expérience confirmée dans une fonction de responsabilité SI.

- Maîtrise de l'administration des infrastructures informatiques, des environnements cloud, des réseaux, des systèmes et des outils collaboratifs.
- Compétences confirmées dans la gestion des identités, des habilitations, des comptes privilégiés et de la sécurisation des accès.
- Bonne maîtrise des dispositifs de cybersécurité, de sauvegarde, de continuité d'activité, de gestion des incidents et de restauration des données.
- Expérience de l'administration technique, de la maintenance et du support des applications métiers et des systèmes de gestion.
- Bonne connaissance des principes de protection des données, de gestion documentaire et de conservation des informations numériques.
- Capacité à diagnostiquer et résoudre des problèmes techniques, à organiser le support aux utilisateurs et à coordonner des interventions spécialisées.
- Expérience du pilotage de prestataires informatiques, du suivi des engagements de service et de la gestion des contrats et licences.
- Maîtrise des outils de gestion de projets, de documentation technique et de reporting.
- Expérience des projets de transformation numérique, de modernisation des infrastructures ou de migration de systèmes appréciée.
- Expérience dans une organisation internationale, multisite ou financée par des bailleurs appréciée.
- Français et anglais professionnels indispensables.
- Rigueur, autonomie technique, sens du service, confidentialité, intégrité, réactivité et capacité d'alerte.

11. Comment postuler

- Veuillez envoyer votre CV et votre lettre de motivation à l'adresse : recruitments@uclg-africa.org
- Date limite : 19 novembre 2026
- Poste basé à Rabat.