



CHARTRE DE VISIBILITÉ NUMÉRIQUE
Présidente du Conseil d'Administration
Autorité institutionnelle

(Document stratégique, Gouvernance de l'image publique)

1. Statut institutionnel de la PCA et enjeux de visibilité numérique

La Présidente du Conseil d'Administration, Madame **Marie Karumba**, incarne une autorité de gouvernance publique investie par décision du Chef de l'État. À ce titre, sa parole, son image et sa présence en ligne ne relèvent pas du registre personnel, mais bien du **registre institutionnel de l'État**.

Dans l'écosystème numérique actuel, la PCA est exposée à des risques élevés d'usurpation d'identité, de manipulation informationnelle et de récupération politique.

L'absence d'un cadre clair de visibilité numérique favorise la prolifération de comptes fictifs parlant en son nom. Il devient donc stratégique de traiter la visibilité numérique de la PCA comme un **actif institutionnel sensible**.

Cette charte vise à établir une **doctrine officielle de présence numérique de la PCA**, au même titre que les règles protocolaires et de communication d'État.

2. Principe fondamental : la PCA comme marque institutionnelle d'État

La PCA ne doit pas être perçue comme une personnalité numérique ordinaire, mais comme une **marque institutionnelle régulée**.

Son nom, son image, sa fonction et sa parole constituent des éléments protégés de l'autorité publique.

Toute utilisation numérique de son identité doit être strictement encadrée, autorisée et traçable.

La PCA ne communique pas pour elle-même, mais au nom de la mission de gouvernance qui lui est confiée. Cette approche permet de dissocier clairement la vie privée de la fonction institutionnelle. Elle impose une gestion professionnelle, centralisée et certifiée de tous les canaux numériques.

3. Audit intégral de l'identité numérique de la PCA

Un audit spécifique et indépendant devra être conduit exclusivement sur l'identité numérique de la PCA.

Cet audit portera sur tous les comptes, pages, profils et contenus utilisant son nom, sa photo ou sa fonction. Il inclura les plateformes sociales, les moteurs de recherche, les blogs et les médias numériques.

Chaque occurrence sera analysée selon son origine, son intention et son degré de nuisance ou de légitimité.

Une cartographie complète de l'empreinte numérique de la PCA sera produite. Ce travail constituera la base stratégique pour la suppression des comptes fictifs et la certification des comptes authentiques.

4. Tolérance zéro envers les comptes fictifs et usurpateurs

Aucun compte non autorisé ne devra subsister dans l'écosystème numérique portant l'identité de la PCA.

Les comptes fictifs constituent une atteinte directe à l'autorité de l'État et à la crédibilité institutionnelle.

Ils favorisent la désinformation, la manipulation de l'opinion et les risques réputationnels.

Une politique de **tolérance zéro** sera appliquée, sans distinction d'audience ou d'ancienneté.

Chaque compte frauduleux devra être signalé officiellement et suivi jusqu'à sa suppression effective.

La PCA ne reconnaîtra publiquement que les comptes certifiés comme étant authentiques.

5. Architecture officielle et unique des comptes de la PCA

La PCA devra disposer d'un nombre limité et strictement contrôlé de comptes institutionnels.

Chaque compte sera créé exclusivement pour un usage officiel, avec une dénomination standardisée. Les plateformes prioritaires seront sélectionnées selon leur crédibilité institutionnelle et leur portée stratégique. Aucun doublon, aucune page parallèle, aucun compte « de soutien » ne sera toléré.

Les comptes officiels devront se référencer mutuellement afin de renforcer leur authenticité.

Cette architecture vise à instaurer une **unicité de la parole numérique de la PCA**.

6. Certification obligatoire et systématique des comptes de la PCA

La certification constitue le **socle non négociable** de la visibilité numérique de la PCA. Tous les comptes et pages institutionnels devront impérativement obtenir un badge de vérification officiel.

La certification permet d'authentifier formellement l'identité de la PCA auprès du public et des partenaires. Elle constitue un mécanisme de protection contre l'usurpation et les fake news. Les démarches de certification devront être portées au nom de la fonction et non de la personne privée.

Aucun compte non certifié ne devra publier de contenu lié à la fonction de PCA.

7. Doctrine de prise de parole numérique de la PCA

La parole numérique de la PCA est une parole institutionnelle engageant l'État. Chaque publication doit être mesurée, stratégique et conforme aux valeurs républicaines. La PCA ne réagit pas à chaud, ne polémique pas et ne répond pas aux attaques numériques.

La communication doit privilégier l'information, la pédagogie et la symbolique institutionnelle.

Les messages doivent être rares, mais à forte valeur institutionnelle. La certification renforce la portée et la solennité de chaque prise de parole.

8. Cellule restreinte de gestion de l'image numérique de la PCA

Une cellule dédiée, restreinte et hautement confidentielle devra être instituée. Cette cellule agira exclusivement pour la PCA et distinctement de toute autre entité. Elle sera chargée de la gestion, de la sécurité et de la cohérence des comptes certifiés. Les accès seront limités, nominatifs et formalisés par écrit.

Toute action numérique devra être documentée et archivée. Cette cellule constitue le garant opérationnel de la doctrine numérique de la PCA.

9. Sécurité renforcée et protection de l'autorité numérique

Les comptes de la PCA doivent être considérés comme des comptes sensibles. Un niveau de sécurité élevé devra être appliqué sans exception. L'authentification forte, la gestion centralisée des accès et la surveillance active sont obligatoires. Tout incident devra être immédiatement signalé et traité. La certification facilite les procédures de récupération en cas de compromission. La protection numérique participe directement à la protection de l'autorité institutionnelle.

10. Suivi stratégique et maîtrise de l'influence institutionnelle

La visibilité numérique de la PCA devra être évaluée de manière stratégique et non quantitative uniquement. L'objectif n'est pas la popularité, mais la crédibilité et l'autorité. Des rapports périodiques analyseront la perception publique, les risques et les opportunités. Les tendances numériques seront anticipées pour éviter les crises réputationnelles.

La stratégie pourra être ajustée selon le contexte institutionnel. La certification demeurera un critère permanent de légitimité et de reconnaissance officielle.

11. Analyse ciblée, Observations méthodologiques générales

11.1 Analyse du compte Facebook

URL analysée : <https://www.facebook.com/marie.karumba>

Il convient, en premier lieu, de vérifier avec la plus grande attention la photo de profil et la photo de couverture du compte. L'utilisation d'un portrait officiel de la PCA ou d'un visuel administratif constitue un indicateur de positionnement institutionnel. À défaut, toute divergence (recadrage approximatif, filigrane absent, qualité faible ou image non officielle) devra être relevée, car elle peut indiquer un compte personnel ou non autorisé.

La section « À propos » doit être examinée en détail afin d'identifier la présence du nom complet, du titre exact de *Présidente du Conseil d'Administration*, de coordonnées professionnelles vérifiables (adresse électronique institutionnelle, numéro professionnel) ainsi que d'un lien vers un site officiel. L'absence de références institutionnelles explicites constitue un point de fragilité notable.

L'historique des publications doit être analysé selon une logique institutionnelle : une autorité publique diffuse principalement des communiqués, comptes rendus d'activités officielles, images protocolaires et messages à caractère administratif. La présence de contenus personnels, d'opinions partisans ou de publications non sourcées doit être considérée comme non conforme.

Les mentions et identifications (tags) associées au compte doivent être contrôlées afin d'identifier la nature des comptes interagissant avec la page. Des interactions majoritairement issues de pages officielles renforcent la légitimité, tandis que des tags provenant de comptes tiers non institutionnels appellent à vigilance.

L'analyse de l'audience et de l'engagement (volume d'abonnés, nature des commentaires, partages, réactions) permet d'évaluer la crédibilité du compte. Un faible engagement pour un compte censé représenter une haute autorité peut indiquer un compte inactif, récent ou non reconnu.

Il est impératif d'exiger, en cas de revendication de contrôle du compte par la PCA, une preuve formelle d'administration : captures d'écran des paramètres de rôles ou confirmation d'accès via une adresse institutionnelle. À défaut, le compte doit être considéré comme non maîtrisé.

Enfin, la présence ou non d'un badge de vérification doit être constatée. En l'absence de certification, une procédure de vérification via les mécanismes de Meta devra être priorisée. Toutes les preuves (captures, dates, URLs) doivent être archivées dans un dossier sécurisé et horodaté.

11.2 Analyse du compte X

URL analysée : <https://x.com/KarumbaMarie>

L'analyse commence par la vérification du nom d'utilisateur, du nom affiché, de la photographie de profil et de la biographie. Une biographie institutionnelle doit mentionner le titre exact, l'année de nomination et, idéalement, un lien vers une source officielle. Toute biographie personnelle ou incomplète constitue un signal d'alerte.

Les publications récentes doivent être examinées quant à leur ton et à leur contenu. Une communication institutionnelle se limite à des communiqués, des extraits de discours, des annonces officielles ou des images d'activités publiques. Les réponses agressives, les prises de position partisans ou les partages de contenus controversés doivent être signalés.

Le statut d'abonnement (X Premium ou équivalent) doit être identifié, la coche bleue étant désormais liée à des offres payantes. Il est essentiel de distinguer une certification institutionnelle d'un simple abonnement individuel.

L'existence d'interactions avec d'autres comptes gouvernementaux ou institutionnels renforce la crédibilité du compte. À l'inverse, l'absence totale de telles interactions affaiblit sa légitimité.

La date de création du compte et l'historique des premiers tweets doivent être comparés à la chronologie réelle de la fonction exercée. Un décalage important constitue un indice potentiel d'usurpation.

En cas d'absence d'accès par la PCA, une procédure de signalement pour usurpation devra être engagée auprès de X, avec constitution préalable d'un dossier de preuves complet.

11.3 Analyse du compte Instagram

URL analysée : <https://www.instagram.com/marie.karumba/>

La photo de profil, la biographie et le lien externe doivent refléter sans ambiguïté le caractère institutionnel du compte. Une mention explicite de la fonction et un renvoi vers un site officiel sont requis.

Le type de contenus publiés (photos, reels, stories) doit correspondre aux usages institutionnels : images protocolaires, vidéos d'événements officiels, communiqués visuels. Un contenu excessivement personnel ou de type « lifestyle » doit être réévalué.

La qualité visuelle est un critère central de crédibilité institutionnelle. Des visuels de faible qualité ou non harmonisés affaiblissent l'image de l'Autorité.

La présence ou non d'un badge de vérification doit être relevée. En cas d'absence, un dossier de demande officielle devra être constitué, incluant les preuves d'identité institutionnelle et la notoriété publique.

L'analyse des commentaires et de la modération permet d'évaluer le sérieux du compte. Une modération inexistante ou incohérente est incompatible avec une fonction d'autorité publique.

11.4 Analyse du second compte Instagram

URL analysée : <https://www.instagram.com/mkbase8/>

Ce compte doit être clairement catégorisé : personnel, compte de soutien, fanpage ou compte potentiellement usurpateur. L'analyse de la biographie, du nom et du contenu permet de déterminer son statut réel.

Si le compte ne reflète pas directement l'activité institutionnelle de la PCA, il doit être officiellement dissocié de l'écosystème institutionnel. Toute diffusion d'informations erronées ou sensibles doit faire l'objet d'un retrait immédiat.

Lorsque le compte agit sans autorisation mais sans intention nuisible, une réaffectation encadrée peut être envisagée. En revanche, en cas de risque réputationnel ou juridique, une procédure de signalement doit être enclenchée.

12. Directives opérationnelles pour l'adaptation des comptes à une autorité de l'État

- Ces directives constituent :
- Un référentiel de gouvernance numérique ;
- Un socle de conformité institutionnelle ;
- Un outil de sécurisation juridique et réputationnelle de la fonction de PCA.

Conclusion institutionnelle

Le présent document établit un cadre clair d'analyse, de décision et d'action relatif à la présence numérique de la Présidente du Conseil d'Administration. Il vise à garantir l'authenticité, la sécurité, la cohérence et la crédibilité de la communication institutionnelle, dans le respect des standards internationaux et des exigences propres à une autorité de l'État.

13. Budget prévisionnel et responsabilité de mise en œuvre

La mise en conformité de la visibilité numérique de la Présidente du Conseil d'Administration constitue une **opération institutionnelle stratégique** engageant la crédibilité, la sécurité et l'autorité de l'État dans l'espace numérique. À ce titre, les dépenses y afférentes ne relèvent ni d'un budget de communication ordinaire ni d'initiatives ponctuelles, mais bien d'un **budget de protection et de légitimation institutionnelle**.

Le budget prévisionnel couvre l'ensemble du cycle de mise en œuvre : audit, constitution des preuves, certification officielle des comptes, sécurisation technique, production de contenus institutionnels et, le cas échéant, actions juridiques de purge et de signalement. Chaque dépense est directement liée à une exigence de gouvernance numérique et répond à un objectif de réduction des risques d'usurpation, de désinformation et de perte d'autorité.

La responsabilité de la mise en œuvre budgétaire incombe à la **cellule restreinte de gestion de l'image numérique de la PCA**, sous la supervision hiérarchique du Cabinet ou de l'organe compétent. Aucune dépense ne pourra être engagée sans traçabilité administrative, justification fonctionnelle et validation formelle.

Les coûts présentés ci-dessous sont des **estimations prudentes**, adaptées au contexte opérationnel de Kinshasa, et devront être ajustés selon les procédures internes de passation et de contrôle.

Ce budget doit également prévoir une **vision récurrente**, afin d'assurer la continuité de la certification, de la sécurité et de la surveillance stratégique dans le temps.

Enfin, le non-financement de ces actions expose la PCA et l'institution à des risques réputationnels majeurs, dont le coût politique et institutionnel serait largement supérieur aux investissements préventifs proposés.

Tableau Budget prévisionnel de certification et de mise en conformité numérique de la PCA

N°	Poste budgétaire	Description détaillée	Quantité	Coût unitaire (USD)	Coût total (USD)
1	Audit et cartographie numérique	Recensement des comptes, captures, preuves, qualification des profils, rapport écrit	Forfait	600	600
2	Montage des dossiers de certification	Constitution des dossiers Meta et X (documents, lettres officielles, suivi)	Forfait	800	800
3	Abonnement Meta Verified	Facebook & Instagram (web) facilitation du support et de la vérification	2 comptes × 12 mois	136	1632
4	Abonnement X Premium	Vérification du compte institutionnel X (tarif web indicatif)	1 compte × 1 an	490	490
5	Production de contenus institutionnels	Photos officielles, visuels normalisés, vidéos courtes protocolaires	Forfait	700	700
6	Sécurisation technique des comptes	Clés de sécurité (FIDO2), gestionnaire de mots de passe institutionnel	Forfait	120	120
7	Formation et encadrement du Community Manager	Formation en communication institutionnelle et diplomatie numérique	Forfait	300	300
8	Actions juridiques et signalements	Rédaction lettres officielles, mise en demeure, suivi contentieux	Forfait	1500	1500

9	Communication de légitimation officielle	Publications sponsorisées annonçant les comptes authentifiés	Forfait	800	800
10	Provision pour imprévus (10 %)	Couverture des frais non anticipés	—	—	345

Total prévisionnel estimé : 7.287 USD