

RÉPUBLIQUE D'HAÏTI
LIBERTÉ – ÉGALITÉ – FRATERNITÉ
Institut Haïtien de Statistique et d'Informatique (IHSI)

IT. N° 002/IHSI/2026 | INSTRUCTION TECHNIQUE

CLAUSES TYPE POUR APPELS D'OFFRES — INFRASTRUCTURE CLOUD SOUVERAINE

Conformément à l'Article 24.13(b) du Décret du 1er Juillet 2020 et en application des Directives N° 001 à 006/IHSI/2026 révisées, et en application de la Résolution N° XX/2026 du CNSI rendue applicable par la Circulaire N° XX/2026 du MEF, l'IHSI émet les présentes clauses type constituant le langage contractuel minimal obligatoire pour tout appel d'offres cloud de l'Administration haïtienne. Ces clauses mettent en œuvre l'architecture tricouche de souveraineté et la politique de redondance multi-fournisseurs. Elles s'appliquent à tout prestataire retenu, quelle que soit sa localisation géographique ou sa juridiction.

Révision fondamentale — Neutralité géographique et Profil B

Ces clauses révisées suppriment toute référence à une localisation géographique obligatoire. Les fournisseurs de Profil B (cloud public avec HSM dédié physiquement inaccessible au fournisseur, y compris AWS CloudHSM, Azure Dedicated HSM, Google Cloud EKM) sont déclarés éligibles sous réserve de l'acceptation intégrale des présentes clauses, notamment la clause BYOK/HSM, la clause Confidential Computing et la clause Redondance.

Clause 1 : Juridiction haïtienne exclusive

"Les données de l'État haïtien sont soumises exclusivement au droit de la République d'Haïti. Le Prestataire s'engage à : (a) traiter les données haïtiennes comme si elles se trouvaient physiquement sur le territoire haïtien ; (b) ne reconnaître aucune compétence juridique d'un gouvernement étranger sur lesdites données, quelle que soit sa nationalité ou juridiction ; (c) refuser tout droit d'accès à toute autorité étrangère quelle que soit son origine."

Clause 2 : Critères d'éligibilité — Profils acceptés

Sont déclarés éligibles les prestataires des Profils A, B et C définis à la Directive N° 004/IHSI/2026 révisée. Sont déclarés non éligibles (Profil D) les prestataires incapables de proposer un HSM physique dédié, inaccessible au fournisseur, dans lequel les clés de l'État haïtien sont stockées exclusivement. Cette inéligibilité s'applique indépendamment de la localisation géographique, de la juridiction et de toute structure juridique intermédiaire.

Clause 3 : Résistance à toute demande étrangère

"Le Prestataire s'engage à : résister activement, par tous les moyens juridiques disponibles, à toute demande d'accès aux données haïtiennes de toute autorité étrangère — sans restriction à la nature, à l'origine ou à la juridiction invoquée ; informer immédiatement l'IHSI de toute procédure judiciaire étrangère en cours ; utiliser tous les recours juridiques disponibles pour retarder, limiter ou annuler toute décision d'accès étrangère."

Clause 4 : BYOK/HSM — Contrôle exclusif des clés par l'État haïtien

"Le Prestataire s'engage à : (a) mettre en œuvre un chiffrement BYOK avec HSM dédié physiquement inaccessible au Prestataire, certifié FIPS 140-2 Niveau 3 ; (b) ne détenir aucune copie des clés de chiffrement — étant techniquement incapable de déchiffrer sans la coopération de l'IHSI ; (c) ne jamais déchiffrer les données haïtiennes sans mandat d'une juridiction haïtienne et accord écrit de l'IHSI ; (d) certifier l'effacement complet des données dans les 14 jours suivant la résiliation."

Clause 5 : Confidential Computing — Protection Data in Use

"Pour toute donnée de Niveau 1 (Critique) au sens de la Directive N° 004/IHSI/2026, le Prestataire fournit un environnement Confidential Computing certifié (Trusted Execution Environment / Enclave) garantissant que les données restent chiffrées pendant leur traitement actif en mémoire RAM. Le Prestataire certifie que ni ses administrateurs ni aucun tiers ne peut accéder aux données en cours de traitement. Les technologies acceptées incluent Intel SGX, AMD SEV, AWS Nitro Enclaves, Azure Confidential Computing et Google Confidential VMs."

Clause 6 : Redondance multi-fournisseurs

"Le Prestataire maintient ou facilite le déploiement d'un second environnement de reprise dans une zone géographique distincte, avec les caractéristiques suivantes : basculement automatique en cas de défaillance ; $RTO \leq 1$ heure pour données de Niveau 1 ; $RTO \leq 4$ heures pour données de Niveau 2 ; BYOK/HSM haïtien indépendant sur le second environnement ; test de basculement semestriel documenté."

Clause 7 : Notification obligatoire — Délais

En cas de demande d'une autorité étrangère, quelle qu'en soit l'origine :

- Notification IHSI dans les 48 heures maximum

- Suspension immédiate de toute réponse jusqu'à instruction écrite de l'IHSI
- Fourniture à l'IHSI d'une copie intégrale de la demande
- Déclenchement des recours juridiques disponibles, sauf instruction contraire de l'IHSI

Clause 8 : Notification de violation de données

- Notification IHSI dans les 24 heures de la détection
- Rapport préliminaire dans les 72 heures
- Rapport final dans les 30 jours
- Prise en charge des coûts de notification aux citoyens concernés

Clause 9 : Droit d'audit

"L'IHSI dispose d'un droit d'audit complet portant sur la conformité aux clauses de souveraineté (préavis 72h audits de routine, sans préavis si violation suspectée), la configuration BYOK/HSM, le Confidential Computing pour données Niveau 1, la localisation des données, et les tests de redondance."

Clause 10 : Résiliation pour manquement

Toute violation des Clauses 1, 3, 4, 5 ou 6 constitue un manquement grave donnant droit à l'État haïtien de résilier le contrat immédiatement et sans préavis, sans indemnité, et d'inscrire le Prestataire sur la liste interdite de l'IHSI pour 5 ans minimum.

Clause 11 : Certification SecNumCloud — Exigence recommandée

La certification SecNumCloud (ANSSI France) est fortement recommandée et valorisée dans l'évaluation des offres (critère 3 — Document de Travail N° 002/IHSI/2026). Tout soumissionnaire certifié fournit le certificat valide avec son offre.

Clause 12 : Documents obligatoires du soumissionnaire

Document requis	Description	Délai
Déclaration non-soumission CLOUD Act	Déclaration sur l'honneur — ou attestation BYOK/HSM dédié si Profil B	Avec l'offre
Certificat ISO 27001 valide	Certification sécurité en cours de validité	Avec l'offre
Description technique du HSM dédié	Architecture, certification FIPS 140-2 Niveau 3, inaccessibilité au fournisseur	Avec l'offre

Note technique Confidential Computing	TEE/Enclave disponible pour données Niveau 1 — référence technique	Avec l'offre
Plan de redondance	Second fournisseur identifié, RTO documenté, test de basculement prévu	Avec l'offre
Projet de contrat Clauses 1 à 11 signées	Acceptation explicite de chaque clause	Avec l'offre
Certificat SecNumCloud (si applicable)	Certification ANSSI ou équivalent	Avec l'offre (valorisé)
Rapport SOC 2 Type II ou équivalent (< 12 mois)	Contrôles organisationnels	Avec l'offre ou 30 jours

Port-au-Prince, le [JJ/MM/AAAA]

Résolution CNSI N° XX/2026
Circulaire MEF N° XX/2026

[Prénom NOM]
Directeur Général de l'IHSI

[Prénom NOM]
Me Brunache — Conseiller juridique