

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

Dir. N° 004/IHSI/2026 | DIRECTIVE

POLITIQUE DE SOUVERAINETÉ DES DONNÉES NUMÉRIQUES DE L'ÉTAT HAÏTIEN

Conformément à l'Article 24.13 du Décret du 1er Juillet 2020, et en application de la Résolution N° XX/2026 du CNSI rendue applicable par la Circulaire N° XX/2026 du MEF, l'IHSI émet la présente Politique de souveraineté révisée. La souveraineté haïtienne est définie par le contrôle exclusif des clés BYOK/HSM — non par la localisation géographique. La présente Directive adopte une architecture tricouche : juridique (juridiction haïtienne), technique au repos (BYOK/HSM), et technique en traitement (Confidential Computing).

Article 1 : Définition de la souveraineté — Architecture tricouche

La souveraineté des données s'entend comme le contrôle juridique et technique exclusif de l'État haïtien sur ses données numériques, indépendamment de la localisation physique des serveurs et de la juridiction du fournisseur.

Point fondamental — Le CLOUD Act ne compromet pas la souveraineté haïtienne avec BYOK/HSM

Un fournisseur soumis au CLOUD Act (AWS, Azure, Google) peut être utilisé. Si un gouvernement étranger exige la remise de données haïtiennes, le fournisseur livrera des données chiffrées AES-256 illisibles — les clés de déchiffrement étant dans le HSM haïtien, hors de portée du fournisseur. C'est l'équivalent de livrer un coffre-fort sans la combinaison.

Couche 1 — Protection juridique : Juridiction haïtienne exclusive

- Seul le droit de la République d'Haïti est applicable aux données numériques de l'État haïtien
- Le prestataire résiste activement à toute demande d'accès de toute autorité étrangère — y compris les autorités du pays hôte
- Notification IHSI dans les 48 heures de toute demande étrangère + suspension immédiate de toute réponse

Couche 2 — Data at Rest et Data in Transit : BYOK/HSM haïtien

Toutes les données de l'État haïtien sont chiffrées AES-256 avec des clés exclusivement sous contrôle haïtien. Le prestataire cloud ne détient aucune copie des clés — il est techniquement incapable de déchiffrer les données haïtiennes, même sous injonction d'un tribunal étranger.

Couche 3 — Data in Use : Confidential Computing

Pour les données de Niveau 1, les traitements actifs en mémoire RAM sont protégés par des Trusted Execution Environments (TEE). Les données restent chiffrées même pendant leur traitement — inaccessibles même aux administrateurs du fournisseur.

Article 2 : Champ d'application

- Les ministères et organismes autonomes de la République d'Haïti
- L'IHSI et les entités du SyNSIP (Article 8 du Décret du 1er Juillet 2020)
- Les collectivités territoriales
- Tout prestataire ou sous-traitant agissant pour le compte de l'État haïtien

Classification des données et exigences d'infrastructure

La présente classification détermine le type d'infrastructure cloud obligatoire pour chaque catégorie de données de l'État haïtien. Elle s'applique indépendamment de la localisation géographique des serveurs.

Niveau	Données concernées	Infrastructure	BYOK/HSM	Data in Use
NIVEAU 1 CRITIQUE	Biométrie (empreintes, facial, iris) Identité (CIN, passeport, NIN, acte naissance) Données fiscales personnelles (DGI) Dossiers médicaux (MSPP) Données judiciaires (MJSP) Sécurité nationale et défense Données électorales (ONI) Clés cryptographiques de l'État	Bare metal dédié OBLIGATOIRE (serveur physique exclusif)	OBLIGATOIRE HSM physique FIPS 140-2 Niv. 3 sous contrôle haïtien exclusif	OBLIGATOIRE Confidential Computing (TEE/Enclave certifié)
NIVEAU 2 SENSIBLE	Personnel fonction publique (OMRH) Marchés publics et contrats Budgets internes non publiés Correspondances classifiées Données statistiques brutes (IHSI)	Bare metal RECOMMANDÉ Cloud public avec HSM dédié ACCEPTABLE	OBLIGATOIRE HSM dédié chez fournisseur (CloudHSM AWS, Azure Dedicated HSM, Google CloudHSM)	RECOMMANDÉ Zero Trust + journalisation

	Serveurs de messagerie (@gouv.ht)			
NIVEAU 3 INTERNE	Emails courants agents .gouv.ht Documents travail non classifiés Agendas et calendriers Rapports d'activité internes	Cloud public ACCEPTABLE (AWS, Azure, Google, CloudCarib ou équivalent) avec BYOK obligatoire	OBLIGATOIRE BYOK via services cloud (Customer Key Microsoft, Google EKM, AWS KMS BYOK)	RECOMMANDÉ
NIVEAU 4 PUBLIC	Publications statistiques officielles Textes législatifs publiés au Moniteur Rapports annuels publics Open data gouvernemental	Tout cloud approuvé par l'IHSI	OPTIONNEL	OPTIONNEL

Définition — Bare metal (cloud privé dédié)

Un serveur bare metal est un serveur physique dédié exclusivement à une seule organisation. Aucun autre client ne partage ce matériel. C'est obligatoire pour les données de Niveau 1 car il élimine les risques liés à la mutualisation des ressources physiques.

Principe de neutralité géographique

La souveraineté haïtienne est définie par le contrôle exclusif des clés BYOK/HSM — et non par la localisation des serveurs. Un fournisseur soumis au CLOUD Act (AWS, Azure, Google) est acceptable si les clés de déchiffrement restent exclusivement dans un HSM haïtien inaccessible au fournisseur. Même sous injonction CLOUD Act, le fournisseur ne peut livrer que des données chiffrées illisibles.

Exigence de redondance multi-fournisseurs

Un prestataire cloud unique constitue un point de défaillance unique inacceptable pour une infrastructure gouvernementale. L'État haïtien maintient au minimum deux fournisseurs cloud approuvés dans des zones géographiques distinctes.

Exigence	Standard minimal	Justification
Nombre de fournisseurs	Minimum 2 fournisseurs approuvés par l'IHSI, actifs simultanément	Éliminer le Single Point of Failure
Séparation géographique	Zones géographiques distinctes (ex. : caribéen + nord-américain ou européen)	Protection contre catastrophes naturelles et coupures régionales
RTO Niveau 1	≤ 1 heure — basculement automatique	Continuité services publics critiques
RTO Niveau 2	≤ 4 heures	Continuité services administratifs
RTO Niveau 3	≤ 24 heures	Reprise normale

Clés HSM	HSM indépendants chez chaque fournisseur — clés non partagées	Compromission d'un HSM n'affecte pas l'autre
Fournisseurs acceptables	CloudCarib, OVHcloud, IONOS, AWS (CloudHSM), Azure (Dedicated HSM), Google Cloud (EKM)	Liste mise à jour annuellement par l'IHSI

Profils de prestataires cloud — Critères d'éligibilité

L'éligibilité d'un prestataire est déterminée par ses capacités techniques de souveraineté — non par sa localisation géographique.

Profil	Caractéristiques	Exemples	Niveaux	Statut
Profil A BARE METAL SOVERAIN	Serveurs physiques dédiés (bare metal) ISO 27001 obligatoire HSM physique dédié FIPS 140-2 Niv. 3 BYOK natif — fournisseur sans accès aux clés Confidential Computing disponible Engagement contractuel de résistance à toute demande étrangère	OVHcloud, IONOS, Hetzner CloudCarib, C3 Caraïbes	Tous niveaux	AUTORISÉ PROFIL DE RÉFÉRENCE
Profil B CLOUD PUBLIC SOVERAIN	Cloud public mutualisé ISO 27001 obligatoire HSM DÉDIÉ chez fournisseur (physiquement inaccessible au fournisseur) BYOK — fournisseur sans accès aux clés Confidential Computing disponible Peut être soumis au CLOUD Act Clauses contractuelles notification 48h obligatoires	AWS (CloudHSM) Azure (Dedicated HSM) Google Cloud (EKM + Confidential VM)	Niveaux 2, 3, 4 (Niveau 1 avec Confidential Computing obligatoire)	AUTORISÉ sous conditions BYOK/HSM dédié
Profil C CLOUD CARAÏBE SOVERAIN	Fournisseur caribéen certifié ISO 27001 BYOK disponible Non soumis au CLOUD Act Latence réduite depuis Haïti Recommandé comme fournisseur de redondance	CloudCarib (Curaçao) C3 (Barbade) Equinix Caribbean	Tous niveaux (selon capacité HSM)	AUTORISÉ RECOMMANDÉ pour redondance
Profil D INTERDIT	Fournisseur sans HSM dédié indépendant Clés gérées par le fournisseur Données accessibles en clair au fournisseur	Tout fournisseur sans BYOK/HSM dédié	AUCUN	INTERDIT éliminatoire

Article 6 : Obligations contractuelles obligatoires

Clause	Libellé contractuel obligatoire
--------	---------------------------------

Juridiction haïtienne exclusive	"Les données de l'État haïtien sont soumises exclusivement au droit haïtien. Le Prestataire traite ces données comme si elles se trouvaient physiquement en Haïti, quelles que soient les lois du pays hôte."
Résistance aux autorités étrangères	"Le Prestataire résiste, par tous moyens juridiques, à toute demande d'accès de toute autorité étrangère, quelle que soit sa nationalité ou juridiction."
Notification 48 heures	"En cas de demande étrangère, le Prestataire notifie l'IHSI dans les 48 heures et suspend toute réponse jusqu'à instruction contraire de l'IHSI."
BYOK/HSM	"Les clés AES-256 sont exclusivement contrôlées par l'État haïtien via HSM dédié. Le Prestataire ne détient aucune copie."
Confidential Computing	"Pour les données de Niveau 1, le Prestataire fournit un environnement TEE/Enclave garantissant que les données restent chiffrées pendant leur traitement en mémoire RAM."
Redondance	"Le Prestataire maintient un second environnement dans une zone géographique distincte avec basculement automatique ≤ 1 heure pour données Niveau 1."
Droit d'audit et réversibilité	"L'IHSI peut auditer le Prestataire sur préavis de 72 heures. En cas de résiliation, données exportables sous 14 jours, puis effacement certifié."

Article 7 : Sanctions

La violation de la présente Directive expose l'institution aux sanctions de l'Article 28 du Décret du 1er Juillet 2020. Toute violation des clauses de souveraineté par le prestataire entraîne la résiliation immédiate sans indemnité et l'inscription sur la liste interdite de l'IHSI pour 5 ans minimum.

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