RÉPUBLIQUE D'HAÏTI

LIBERTÉ – ÉGALITÉ – FRATERNITÉ

Institut Haïtien de Statistique et d'Informatique (IHSI)

Dir. N° 006/IHSI/2026 | DIRECTIVE

ARCHITECTURE DE SOUVERAINETÉ NUMÉRIQUE POUR L'HÉBERGEMENT DES DONNÉES PUBLIQUES HAÏTIENNES

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 Directive remplaçant tout texte antérieur faisant référence à une localisation géographique obligatoire. La souveraineté est définie par le contrôle des clés BYOK/HSM — tout fournisseur cloud approuvé est acceptable quelle que soit sa localisation ou juridiction.

Article 1 : Objet et principe fondateur

La présente Directive établit l'architecture complète de souveraineté numérique pour l'hébergement des données publiques haïtiennes. Le principe fondateur est que la souveraineté haïtienne sur ses données est garantie par le contrôle exclusif des clés de chiffrement BYOK/HSM — et non par la localisation géographique des serveurs. Cette approche permet d'utiliser tout fournisseur cloud approuvé par l'IHSI, quelle que soit sa localisation ou sa juridiction.

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 SOUVERAIN	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	Cloud public mutualisé ISO 27001 obligatoire HSM DÉDIÉ chez fournisseur (physiquement	AWS (CloudHSM) Azure (Dedicated HSM) Google	Niveaux 2, 3, 4 (Niveau 1 avec	AUTORISÉ sous conditions BYOK/HSM dédié

PUBLIC SOUVERAIN	inaccessible au fournisseur) BYOK — fournisseur sans accès aux clés Confidential Computing disponible Peut être soumis au CLOUD Act Clauses contractuelles notification 48h obligatoires	Cloud (EKM + Confidential VM)	Confidential Computing obligatoire)	
Profil C CLOUD CARAÏBE SOUVERAIN	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

Modèle de protection tricouche

La protection des données haïtiennes couvre trois états d'existence numérique. La protection bicouche antérieure était incomplète — elle ignorait les données en cours de traitement actif.

Couche	État	Menace couverte	Standard requis	Obligatoire pour
Couche 1 DATA AT REST	Données stockées sur disque	Accès physique — saisie judiciaire — piratage	Chiffrement AES-256 + BYOK/HSM haïtien HSM FIPS 140-2 Niveau 3	Tous niveaux
Couche 2 DATA IN TRANSIT	Données en circulation réseau	Interception — man-in-the-middle	TLS 1.3 — aucun fallback TLS 1.2 VPN IPsec IKEv2 AES-256-GCM	Tous niveaux
Couche 3 DATA IN USE (NOUVEAU)	Données en traitement actif en mémoire RAM	Memory scraping — cold boot attack — accès administrateur malveillant	Confidential Computing (TEE) : • Azure Confidential Computing (Intel SGX/AMD SEV) • AWS Nitro Enclaves • Google Confidential VMs (AMD SEV) Zero Trust + journalisation accès mémoire Effacement RAM certifié post-traitement	Niveau 1 : OBLIGATOIRE Niveau 2-3 : RECOMMANDÉ

Pourquoi la couche Data in Use est critique

Quand une application traite des données — calculer une fiche fiscale, afficher un dossier médical — ces données existent en clair dans la RAM du serveur. Sans Confidential Computing, un acteur malveillant ayant accès au serveur à cet instant peut intercepter ces données, contournant toutes les protections au repos et en transit. Le Confidential Computing chiffre les données même pendant leur traitement, les rendant illisibles même pour les administrateurs du fournisseur cloud.

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) Serveurs de messagerie (@gouv.ht)	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
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.

Article 5 : Infrastructure de messagerie gouvernementale

Infrastructure de messagerie gouvernementale (@gouv.ht)

Règle spéciale — Serveurs de messagerie (Niveau 2 — Sensible)

Les serveurs de messagerie @gouv.ht sont classifiés Niveau 2 même si les emails individuels sont Niveau 3. L'accès au serveur de messagerie donne accès à l'historique complet des communications de l'État. Infrastructure bare metal dédié RECOMMANDÉE — cloud public avec HSM dédié ACCEPTABLE. Microsoft Exchange Online sur Azure avec Azure Dedicated HSM + Customer Key constitue une solution acceptable (Profil B). Auto-hébergement en Haïti INTERDIT. Services grand public (Gmail, Yahoo, Outlook.com) INTERDITS.

Paramètre	Exigence	Justification
Infrastructure	Bare metal dédié (recommandé) ou cloud public avec HSM dédié (acceptable)	Niveau 2 — Sensible
Chiffrement au repos	AES-256 + BYOK/HSM exclusivement haïtien	Souveraineté des données
Chiffrement en transit	TLS 1.3 — aucun fallback TLS 1.2	Art. 1.m du Décret
MFA	Obligatoire pour TOUS les utilisateurs	Art. 24.10 du Décret
Confidential Computing	Recommandé pour le traitement des emails	Protection Data in Use
Rétention légale	5 ans min. — 10 ans documents financiers	Conformité légale haïtienne
DMARC / DKIM / SPF	Configurables pour tous les domaines .gouv.ht	Authenticité des courriels officiels
Taille de boîte	50 Go minimum par utilisateur — illimité pour Ministres et DG	Rétention légale 10 ans
Redondance	2 fournisseurs approuvés — basculement automatique ≤ 1 heure	Continuité opérationnelle

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

Article 7 : Interprétation — Article 1.g (Conservation)

L'expression « banque nationale de données » de l'Article 1.g s'entend comme incluant toute infrastructure cloud souveraine approuvée par l'IHSI, quelle que soit sa localisation physique, à condition que : (1) les données soient soumises exclusivement au droit haïtien ; (2) les clés de chiffrement soient exclusivement contrôlées par l'État haïtien via HSM dédié ; (3) le prestataire s'engage à résister à toute demande étrangère ; et (4) l'architecture tricouche soit respectée.

Article 8 : Interprétation — Article 1.k (Centre national des données)

L'expression « dispositif technologique » de l'Article 1.k n'implique pas une localisation physique en Haïti. Le Centre national des données s'entend comme l'ensemble des infrastructures cloud souveraines approuvées par l'IHSI, incluant les systèmes de redondance multi-fournisseurs.

Article 9 : Tableau de conformité — Scénarios

Scénario	Sans BYOK/HSM haïtien	Avec BYOK/HSM + Confidential Computing
Tribunal étranger ordonne accès aux serveurs	Données livrées en clair — souveraineté perdue	Données chiffrées AES-256 illisibles — clés en Haïti
Demande CLOUD Act d'une autorité américaine	Si sans BYOK : données accessibles	Fournisseur peut remettre les serveurs — données illisibles sans clés haïtiennes
Prestataire cloud piraté	Données en clair compromises	Données chiffrées AES-256 illisibles
Attaquant accède à la RAM pendant traitement	Données interceptées en mémoire	Données chiffrées par TEE/Enclave — illisibles même en RAM

Prestataire fait faillite — actifs saisis	Données potentiellement accessibles	Données illisibles — clés HSM révoquées par l'IHSI
Panne du fournisseur principal	Perte de service	Basculement automatique ≤ 1 heure vers le second fournisseur

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