RÉPUBLIQUE D'HAÏTI

LIBERTÉ – ÉGALITÉ – FRATERNITÉ

Institut Haïtien de Statistique et d'Informatique (IHSI)

Dir. N° 001/IHSI/2026 | DIRECTIVE

POLITIQUE NATIONALE DE GOUVERNANCE ÉLECTRONIQUE D'HAÏTI

Conformément aux attributions conférées par l'Article 24.13(a) 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 établissant le cadre de gouvernance électronique de l'administration publique haïtienne. La souveraineté numérique est définie par le contrôle exclusif des clés BYOK/HSM — non par la localisation géographique des serveurs.

Article 1 : Objet

La présente Directive établit le cadre de gouvernance électronique pour l'ensemble de l'administration publique haïtienne, en conformité avec l'Article 24.13(a) du Décret du 1er Juillet 2020. La souveraineté numérique est assurée par l'architecture tricouche BYOK/HSM définie à l'Article 5 — indépendamment de la localisation géographique des serveurs.

Article 2 : Champ d'application

- Tous les ministères et organismes autonomes de la République d'Haïti
- Les collectivités territoriales
- Toutes les entités membres du SyNSIP (Article 8 du Décret du 1er Juillet 2020)
- Tout prestataire privé traitant des données pour le compte de l'État haïtien

Article 3 : Principes directeurs

Principe	Description
Centricité citoyenne	Services numériques conçus pour les besoins des citoyens haïtiens (Art. 6 du Décret).
Souveraineté par défaut	Toutes les données publiques sont protégées par l'architecture tricouche BYOK/HSM — la localisation géographique est secondaire à la maîtrise des clés.
Interopérabilité	Systèmes gouvernementaux via normes ouvertes, sous coordination DCSyNSIP (Art. 24.9).

Sécurité et confidentialité	Protection des données conforme aux Articles 1.f, 1.m, 24.10 et 29 du Décret.
Redondance	Toute infrastructure critique déployée chez minimum 2 fournisseurs approuvés.
Inclusion numérique	Accessibilité pour tous les citoyens, y compris en zones rurales (Art. 7.c).
Transparence	Ouverture des données statistiques non confidentielles (Art. 6).

Article 4 : Domaines d'action prioritaires

Domaine	Description	Direction IHSI
Identité numérique	Identifiant unique et sécurisé pour l'accès aux services publics.	DDCT (Art. 24.11)
Digitalisation des services	Priorisation services à fort impact citoyen (Art. 12).	DDCT + Ministères
Partage sécurisé des données	Interconnexion des institutions (Art. 24.9).	DCSyNSIP
Open Data	Accès public aux données gouvernementales non sensibles (Niveau 4).	DCSyNSIP + IHSI
Cybersécurité	Normes obligatoires pour tous les systèmes publics (Art. 24.10).	DIRC
Infrastructure cloud souveraine	Architecture tricouche — prestataire sélectionné par marché public.	IHSI (Art. 24.13)

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	Tout cloud approuvé par l'IHSI	OPTIONNEL	OPTIONNEL

	annuels publics Open data gouvernemental			

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

Article 6 : Clauses contractuelles de souveraineté — Obligatoires

Tout marché public cloud passé par l'État haïtien DOIT inclure :

- Juridiction haïtienne exclusive : seul le droit haïtien s'applique aux données

- BYOK/HSM : clés AES-256 exclusivement sous contrôle haïtien — fournisseur sans accès aux clés
- Notification 48 heures : alerte IHSI de toute demande d'accès étrangère + suspension immédiate
- Confidential Computing : pour données de Niveau 1 — TEE/Enclave certifié requis
- Redondance : 2 fournisseurs actifs — basculement automatique ≤ 1 heure pour Niveau 1
- Droit d'audit : IHSI peut auditer le prestataire sur préavis de 72 heures
- Réversibilité : données exportables sous 14 jours en cas de résiliation

Article 7 : Calendrier de conformité

Étape	Responsable	Délai
Appel d'offres infrastructure cloud souveraine	IHSI	2 mois après signature
Attribution marché public cloud	IHSI + Commission	4 mois après publication
Migration pilote messagerie IHSI	IHSI + prestataire	6 mois après attribution
Migration messagerie tous ministères	Ministères + IHSI	18 mois après attribution
Déploiement Confidential Computing Niveau 1	IHSI + prestataires	24 mois après attribution
Migration complète applications	IHSI + ministères	30 mois après attribution
Audit de conformité complet	IHSI + tiers indépendant	36 mois après signature

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