

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

Dir. N° 003/IHSI/2026 | DIRECTIVE

STANDARDS DE PROTECTION DES DONNÉES NUMÉRIQUES DES CITOYENS

Conformément à l'Article 24.13(d) du Décret du 1er Juillet 2020 mandatant l'IHSI pour définir les standards de protection des données numériques des citoyens, et en référence aux Articles 1.f, 1.m, 2.e et 29 dudit Décret, 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 présents standards inspirés du RGPD et adaptés au contexte juridique haïtien.

Article 1 : Base légale et objet

- Article 24.13(d) : Définir les standards de protection des données numériques des citoyens
- Article 1.f : Données confidentielles — identification directe ou indirecte
- Article 1.m : Cybersécurité — protection contre tout accès non autorisé
- Article 2.e : Secret statistique et utilisation exclusive à des fins statistiques
- Article 29 : Confidentialité absolue des informations nominatives recueillies par l'IHSI

Article 2 : Définitions

Terme	Définition
Donnée citoyenne	Toute information relative à une personne physique identifiée ou identifiable (nom, prénom, adresse, NIN, données de santé, fiscales, éducatives, biométriques, etc.)
Traitement	Toute opération sur des données : collecte, enregistrement, stockage, consultation, utilisation, communication, effacement ou destruction
Responsable de traitement	L'institution publique qui détermine les finalités et les moyens du traitement
Sous-traitant	Le prestataire de services cloud approuvé par l'IHSI, traitant des données pour le compte de l'État haïtien
Violation de données	Toute violation de sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée de données citoyennes

Article 3 : Principes fondamentaux

Principe	Standard	Référence
Licéité	Collecte sur base légale ou consentement explicite du citoyen	Art. 2.e
Finalité	Collecte uniquement pour finalités déterminées — aucune réutilisation incompatible	Art. 2.e
Minimisation	Collecter uniquement les données strictement nécessaires	Art. 24.13.d
Exactitude	Données exactes, complètes et tenues à jour — correction sous 30 jours	Art. 3.d
Conservation limitée	Ne pas conserver au-delà du nécessaire (max 10 ans sauf exception légale)	Art. 24.13.d
Intégrité et confidentialité	Chiffrement AES-256 au repos, TLS 1.3 en transit, RBAC, Confidential Computing Niveau 1	Art. 1.f, 1.m, 29
Responsabilité	Chaque institution démontre sa conformité à la demande de l'IHSI	Art. 24.13.d, e

Article 4 : Droits des citoyens haïtiens

Droit	Mise en œuvre	Délai
Droit d'accès	Copie de ses données (gratuit une fois par an)	30 jours
Rectification	Correction de données inexactes ou incomplètes	30 jours
Effacement	Quand les données ne sont plus nécessaires	60 jours
Limitation	Restreindre le traitement en cas de contestation	15 jours (accusé)
Opposition	S'opposer au traitement pour motifs légitimes	30 jours
Réclamation	Déposer une plainte auprès de l'IHSI (Art. 24.13.e)	Accusé sous 5 jours

Article 5 : Mesures de sécurité techniques minimales

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 6 : Traitement dans l'infrastructure cloud souveraine

Exigence contractuelle	Standard
Juridiction haïtienne exclusive	Prestataire agit exclusivement sur instruction de l'État haïtien
BYOK/HSM haïtien	Clés AES-256 exclusivement sous contrôle haïtien — prestataire sans accès aux clés
Confidential Computing	Obligatoire pour données Niveau 1 — TEE/Enclave certifié
Sous-traitants secondaires	Pré-approuvés par l'IHSI (72h de préavis)
Demandes d'accès étrangères	Notification IHSI dans les 48 heures — suspension immédiate de toute réponse
Suppression des données	Sur demande IHSI, suppression certifiée dans les 14 jours avec rapport d'effacement

Article 7 : Sanctions

La violation des présents standards expose l'institution responsable aux sanctions de l'Article 28 du Décret du 1er Juillet 2020 : amende de 200 000 à 500 000 gourdes ou 2 % du chiffre d'affaires. En cas de récidive : doublement de l'amende. Sanctions disciplinaires pour les agents publics fautifs. Poursuites pénales en cas de violation délibérée du secret statistique (Art. 29).

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