

RÉPUBLIQUE D'HAÏTI

LIBERTÉ – ÉGALITÉ – FRATERNITÉ

Institut Haïtien de Statistique et d'Informatique (IHSI)

NOTE CONCEPTUELLE

CADRE NORMATIF DE LA TRANSFORMATION NUMÉRIQUE
DE L'ADMINISTRATION PUBLIQUE HAÏTIENNE

Directives, Instructions Techniques, Recommandations et Documents de Travail

IHSI / 2026

Référence	NC/IHSI/2026 — Version révisée post-avis Me Brunache
Objet	Vue d'ensemble du dispositif normatif numérique IHSI 2026
Auteur	Direction Générale — Institut Haïtien de Statistique et d'Informatique
Statut	CONFIDENTIEL — Diffusion SyNSIP
Base légale	Décret du 1er Juillet 2020 — Art. 24.13 ; Constitution de 1987
Version initiale	Port-au-Prince, 15 mai 2026
Version révisée	Port-au-Prince, [JJ/MM/AAAA] — Mises à jour §I, §II.2, §II.3

[Prénom NOM]

Directeur Général de l'IHSI

[Prénom NOM]

Conseiller juridique — Me Brunache

I. Introduction et contexte

La présente Note Conceptuelle offre une lecture synthétique et intégrée du corpus normatif émis par l'Institut Haïtien de Statistique et d'Informatique (IHSI) au titre de l'année 2026. Ce corpus constitue le fondement juridique et technique de la transformation numérique souveraine de l'administration publique haïtienne.

Ce travail répond à une obligation légale précise. Le Décret du 1er juillet 2020, en son article 24.13, confère à l'IHSI la mission de définir, publier et diffuser les règles de gouvernance, les normes techniques et les standards applicables à l'ensemble des institutions publiques membres du SyNSIP.

Depuis 2020, aucun cadre normatif contraignant n'avait été publié. Cette absence a produit une dispersion des pratiques, une insécurité juridique pour les responsables d'achats publics, une absence de cadre légal sur la protection des données et une vulnérabilité croissante des systèmes informatiques de l'État.

La présente Note Conceptuelle et les onze instruments qui l'accompagnent comblent ce vide. Ils posent pour la première fois un référentiel unique applicable à toutes les institutions publiques haïtiennes membres du SyNSIP, définissent les règles d'hébergement souverain, protègent les données des citoyens, encadrent la messagerie officielle et organisent la transformation numérique de l'État.

■ Section mise à jour — Version révisée post-avis Me Brunache

■ Mise à jour 1/3 — Statut juridique des instruments et processus de légalisation

À la suite de l'analyse du Décret du 1er Juillet 2020 conduite avec Me Brunache, il est établi que le Décret n'attribue pas expressis verbis à l'IHSI un pouvoir réglementaire général opposable à toute l'administration publique. L'Article 24.13 confère à la DNT un pouvoir normatif TECHNIQUE sectoriel (définir des standards, concevoir des normes, approuver des CDC) — ce qui est différent d'un pouvoir réglementaire général comme celui du Premier Ministre ou d'un Arrêté présidentiel. En conséquence, les onze instruments du présent corpus sont en cours de légalisation via le circuit institutionnel prévu par le Décret lui-même : (1) adoption par Résolution du CNSI (Art. 12 + Art. 15) ; (2) transmission et application par Circulaire du Ministre de l'Économie et des Finances (Art. 16). Ce circuit, décrit dans la Note Stratégique NS/IHSI/2026, confère aux normes IHSI leur pleine opposabilité à toutes les entités du SyNSIP. Les références "Résolution CNSI N° XX/2026" et "Circulaire MEF N° XX/2026" dans chaque instrument seront complétées dès l'adoption par le CNSI.

Face aux contraintes contextuelles — insécurité physique, instabilité électrique, absence d'infrastructure de centres de données conformes aux standards ISO 27001 en Haïti —, l'IHSI a élaboré un modèle de gouvernance électronique souverain ancré sur l'hébergement cloud en Union européenne avec chiffrement BYOK/HSM à clés exclusivement haïtiennes.

Le dispositif normatif se compose de onze (11) instruments répartis en quatre catégories : Directives, Instructions Techniques, Recommandations et Documents de Travail.

II. Architecture du dispositif normatif

2.1 Vue d'ensemble des instruments

Référence	Type	Objet
Dir. N° 001/IHSI/2026	Directive	Politique nationale de gouvernance électronique
Dir. N° 002/IHSI/2026	Directive	Normes techniques — matériels, logiciels et infrastructure cloud souveraine
Dir. N° 003/IHSI/2026	Directive	Standards de protection des données numériques des citoyens
Dir. N° 004/IHSI/2026	Directive	Politique de souveraineté des données numériques de l'État haïtien
Dir. N° 005/IHSI/2026	Directive	Politique d'utilisation de la messagerie électronique
Dir. N° 006/IHSI/2026	Directive	Hébergement des données publiques sur cloud souverain européen
IT. N° 001/IHSI/2026	Instruction Technique	Procédure d'approbation des cahiers des charges techniques (CDC)
IT. N° 002/IHSI/2026	Instruction Technique	Clauses type pour appels d'offres — infrastructure cloud souveraine
Rec. N° 001/IHSI/2026	Recommandation	Standards de mise en œuvre de la signature électronique
NDS. N° 001/IHSI/2026	Note de Service	Plan pilote de migration — messagerie IHSI vers Exchange managé souverain
DT. N° 002/IHSI/2026	Document de Travail	Matrice de décision pour le choix des fournisseurs cloud souverains

2.2 Articulation et hiérarchie normative

■ **Section mise à jour — Version révisée post-avis Me Brunache**

■ Mise à jour 2/3 — Hiérarchie normative enrichie du circuit CNSI/MEF

La hiérarchie pyramidale des instruments est complétée par une couche de validation institutionnelle qui lui confère son opposabilité. Sans cette couche, les instruments ont la valeur de normes techniques internes à l'IHSI. Avec elle, ils deviennent obligatoires pour toutes les entités de l'Administration publique.

Couche	Instruments / Acteurs	Fonction	Opposabilité
Légalisation institutionnelle	Résolution CNSI N° XX/2026 (Art. 12+15) + Circulaire MEF N° XX/2026 (Art. 16)	Adoption officielle + transmission à tous les Ministères et OA	PLEINE — opposable à toutes les entités du SyNSIP
Stratégique	Dir. 001	Cadre de gouvernance électronique nationale	Obligatoire après légalisation CNSI/MEF

Couche	Instruments / Acteurs	Fonction	Opposabilité
Normatif thématique	Dir. 002, 003, 004, 005, 006	Règles sectorielles : technique, données, souveraineté, messagerie, hébergement	Obligatoire après légalisation CNSI/MEF
Opérationnel	IT. 001, IT. 002, NDS. 001	Procédures, clauses contractuelles, plan de migration	Obligatoire dans les marchés publics et approbations IHSI
Conseil / Évaluation	Rec. 001, DT. 002	Signature électronique, matrice de décision cloud	Indicatif (Rec.) / Méthodologique (DT.)

2.3 Format formel des instruments — modèle BRH

■ *Section mise à jour — Version révisée post-avis Me Brunache*

■ Mise à jour 3/3 — Adoption du modèle formel de la Circulaire BRH No. 61-3

Sur recommandation de Me Brunache, le format formel des 11 instruments a été révisé pour adopter le modèle de la Circulaire BRH No. 61-3. Ce modèle supprime les visas formels ("Vu la Constitution... Vu le Décret... Considérant...") et les remplace par un unique paragraphe introductif narratif intégrant directement les références légales pertinentes — plus sobre, plus robuste juridiquement, et cohérent avec la pratique des institutions réglementaires haïtiennes disposant d'un pouvoir normatif sectoriel établi.

Élément	Ancienne formulation (supprimée)	Nouvelle formulation (style BRH)
Préambule	"Vu la Constitution... Vu le Décret... Considérant que... ÉMET LA PRÉSENTE DIRECTIVE :"	Paragraphe introductif unique : "Conformément aux attributions conférées par l'Article 24.13(x) 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 [l'instrument]..."
Entrée en vigueur	"À compter de sa signature par le Directeur Général de l'IHSI"	"À compter de la publication de la Circulaire N° XX/2026 du MEF sur www.ihsi.gouv.ht et sa transmission à tous les Ministères et OA"
Hiérarchie des instruments	Non formalisée	Directive technique / Instruction technique / Recommandation / Note de service / Document de travail — chacun avec portée et fondement distincts

III. Principes fondateurs du cadre normatif

3.1 La souveraineté par défaut

Le principe cardinal du dispositif est la souveraineté numérique de l'État haïtien. Définie à l'Article 1 de la Directive N° 004 comme le « contrôle juridique et technique exclusif et absolu de l'État haïtien sur ses données numériques, indépendamment de la localisation physique des serveurs », elle se décline en deux couches complémentaires :

Couche	Mécanisme	Effet
Couche 1 — Juridique	Juridiction haïtienne exclusive ; engagement contractuel du prestataire à résister à toute demande étrangère, y compris des autorités du pays hôte	Aucune autorité étrangère ne peut obtenir légalement accès aux données haïtiennes
Couche 2 — Technique	Chiffrement AES-256 BYOK/HSM avec clés exclusivement haïtiennes (FIPS 140-2 Niv. 3)	Même en cas d'accès physique ordonné par un tribunal étranger, les données sont illisibles

3.2 L'exclusion des juridictions extraterritoriales

Le dispositif exclut formellement tout prestataire soumis au CLOUD Act américain (Public Law 115-118), au Patriot Act ou à la FISA. Cette exclusion constitue un critère rédhibitoire dans l'évaluation des appels d'offres (Critère 1 — 25 % de la pondération). Elle s'applique indépendamment de toute structure juridique intermédiaire ou coentreprise (voir position IHSI sur Microsoft Bleu — DT. N° 002/IHSI/2026, §4).

3.3 La certification SecNumCloud comme standard de référence

L'IHSI retient la qualification SecNumCloud v3.2+ (ANSSI France) comme critère différenciant de souveraineté dans les marchés publics cloud. Ce référentiel impose au prestataire certifié : l'immunité complète aux lois extraterritoriales, la localisation exclusive des données dans l'UE, le contrôle actionnarial européen et la résistance aux demandes gouvernementales étrangères.

IV. Contenu synthétique des instruments

Directive N° 001 — Gouvernance électronique nationale

Directive fondatrice, elle établit le cadre de gouvernance pour l'ensemble de l'administration publique haïtienne. Elle définit six domaines d'action prioritaires (identité numérique, digitalisation des services, partage de données, Open Data, cybersécurité, infrastructure cloud souveraine), les responsabilités institutionnelles et le calendrier de conformité en huit étapes sur 36 mois.

Directive N° 002 — Normes techniques

Elle standardise les équipements (postes de travail, serveurs), les logiciels approuvés (OS, bureautique, antivirus, bases de données, navigateurs, messagerie) et les exigences de l'infrastructure cloud souveraine. Elle consacre SecNumCloud comme grille d'évaluation et détaille les spécifications IaaS bare metal, Exchange managé et HSM/BYOK.

Directive N° 003 — Protection des données des citoyens

Inspirée des principes du RGPD européen et adaptée au contexte haïtien, elle définit les huit principes fondamentaux (licéité, finalité, minimisation, exactitude, conservation limitée, intégrité, confidentialité, responsabilité), les droits des citoyens (accès, rectification, effacement, opposition) et les mesures de sécurité techniques minimales obligatoires.

Directive N° 004 — Souveraineté des données

Pièce maîtresse du dispositif, elle formalise l'approche bicouche, classe les données par catégorie et exigence de localisation, interdit tout transfert hors Union européenne sans autorisation expresse de l'IHSI, et définit les profils de prestataires autorisés (A/B/C) et interdits (D — soumis au CLOUD Act).

Directive N° 005 — Messagerie électronique

Elle impose l'utilisation exclusive du domaine .gouv.ht pour toutes les communications officielles et prohibe l'utilisation de services grand public (Gmail, Yahoo, Outlook.com). Le service de messagerie doit être un Exchange managé souverain hébergé en UE, avec MFA obligatoire, rétention 5-10 ans et DMARC/DKIM/SPF.

Directive N° 006 — Hébergement cloud souverain européen

Directive interprétative du Décret du 1er Juillet 2020, elle clarifie que l'hébergement en Union européenne est pleinement conforme au cadre légal haïtien. Elle précise que la notion de « banque nationale de données » (Art. 1.g) inclut toute infrastructure sous contrôle juridique et technique exclusif de l'État haïtien, quelle que soit sa localisation physique.

Instruction Technique N° 001 — Approbation des CDC

Elle définit la procédure obligatoire d'évaluation par l'IHSI de tout cahier des charges technique avant développement d'application. Le délai d'instruction est fixé à 23 jours ouvrables. Tout CDC prévoyant un hébergement CLOUD Act, une messagerie grand public ou l'absence de MFA est rejeté

automatiquement.

Instruction Technique N° 002 — Clauses type pour RFP

Elle fournit le langage contractuel minimal obligatoire pour tout appel d'offres cloud de l'administration haïtienne, en 12 clauses couvrant : juridiction haïtienne exclusive, exclusion des prestataires CLOUD Act, résistance à toute autorité étrangère y compris du pays hôte, BYOK/HSM, localisation UE, notification 48h, droit d'audit et résiliation pour manquement.

Recommandation N° 001 — Signature électronique

Elle articule le cadre légal haïtien de la signature électronique (Loi du 14 février 2017, amendée par le Décret du 20 août 2025, et l'Arrêté du 18 septembre 2025) avec le dispositif numérique IHSI. Elle définit les trois niveaux de signature (simple, avancée, qualifiée) et leurs usages gouvernementaux.

Note de Service N° 001 — Plan pilote de migration messagerie

Elle planifie la migration pilote de la messagerie de l'IHSI (200-300 agents) vers le service Exchange managé souverain retenu, en 10 semaines organisées en 4 phases : préparation (S1-S2), implémentation technique (S3-S4), migration par vagues (S5-S8), bascule DNS et désactivation (S9-S10).

Document de Travail N° 002 — Matrice de décision cloud

Outil méthodologique d'aide à la décision pour l'évaluation des offres, il définit 7 critères pondérés : souveraineté/CLOUD Act (25 %), localisation UE (20 %), certifications ISO/SecNumCloud (15 %), Exchange managé (15 %), IaaS bare metal (10 %), engagement contractuel (10 %), prix (5 %).

V. Points clés à retenir

- La souveraineté numérique haïtienne repose sur le chiffrement BYOK/HSM avec clés exclusivement haïtiennes, et non sur la seule localisation physique des serveurs.
- Tout prestataire soumis au CLOUD Act américain est formellement et irrémédiablement exclu des marchés publics cloud haïtiens, indépendamment de toute structure juridique intermédiaire.
- La certification SecNumCloud v3.2+ constitue le critère différenciant de souveraineté dans l'évaluation des offres ; elle est fortement recommandée et génère un bonus significatif.
- L'hébergement cloud européen est juridiquement conforme au Décret du 1er Juillet 2020, tel que clarifié par la Directive N° 006.
- Tout usage de Gmail, Yahoo, Outlook.com ou de tout service de messagerie grand public pour des communications officielles est formellement interdit et passible de sanctions.
- Le SyNSIP dispose de 12 mois après attribution du marché pour migrer l'intégralité de sa messagerie, et de 30 mois pour la migration complète des applications.
- Tout cahier des charges technique doit être soumis à l'IHSI pour approbation avant tout développement, sous peine de rejet automatique des projets non conformes.
- Les 11 instruments sont en cours de légalisation via Résolution CNSI + Circulaire MEF — leur opposabilité pleine et entière est effective dès adoption par le CNSI.

VI. Calendrier de mise en œuvre consolidé

Étape	Délai	Responsable
Adoption des 11 instruments par Résolution du CNSI	J+45 jours	DG IHSI (Secrétaire Exécutif CNSI)
Circulaire MEF transmettant les normes à tous les Ministères	J+60 jours	Ministre de l'Économie et des Finances
Publication de l'appel d'offres cloud souverain	M+2 après signature	IHSI
Attribution du marché public cloud	M+4 après publication	IHSI + Commission
Migration pilote messagerie IHSI (NDS. 001)	M+6 après attribution (10 semaines)	IHSI + prestataire
Migration messagerie — ensemble des ministères	M+18 après attribution	Ministères + IHSI
Migration complète des applications	M+30 après attribution	IHSI + ministères
Audit de conformité complet	M+36 après signature	IHSI + tiers indépendant
Migration signature électronique qualifiée	6 mois après cahier des charges CONATEL	Toutes institutions
Révision des directives	Tous les 2 ans ou si changement majeur	IHSI + CNSI

VII. Régime de sanctions

Le non-respect des présentes directives expose les institutions fautives aux sanctions prévues par le Décret du 1er Juillet 2020 :

Type de violation	Sanction applicable
Violation des standards de protection des données (Dir. 003)	Amende de 200 000 à 500 000 gourdes ou 2 % du CA — Art. 28 du Décret
Violation des clauses de souveraineté par le prestataire (Dir. 004)	Résiliation immédiate sans indemnité + liste interdite IHSI 5 ans
Usage de messagerie non conforme (Dir. 005)	Avertissement → suspension d'accès → sanction disciplinaire → poursuites pénales
CDC non conforme soumis à l'IHSI (IT. 001)	Rejet automatique ; voie de recours : DG IHSI dans 15 jours, puis CNSI
Violation délibérée du secret statistique (Art. 29 du Décret)	Poursuites pénales

VIII. Conclusion

Le dispositif normatif de l'IHSI pour 2026 constitue un corpus cohérent, hiérarchisé et opérationnel, conçu pour doter l'État haïtien d'une transformation numérique souveraine, sécurisée et conforme à ses obligations légales. Il repose sur la conviction que la souveraineté numérique ne se décrète pas — elle se construit, instrument par instrument, clause par clause, clé de chiffrement par clé de chiffrement.

Sa mise en œuvre effective requiert la mobilisation coordonnée de l'IHSI, de ses directions techniques, de l'ensemble des ministères membres du SyNSIP, et des prestataires sélectionnés par appel d'offres public. Le succès du pilote de migration messagerie à l'IHSI constituera le signal concret que la transformation numérique souveraine d'Haïti est engagée.

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

[Prénom NOM]

Directeur Général de l'IHSI

[Prénom NOM]

Conseiller juridique — Me Brunache