

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

Dir. N° 005/IHSI/2026 | DIRECTIVE

POLITIQUE D'UTILISATION DE LA MESSAGERIE ÉLECTRONIQUE

Conformément à l'Article 24.13(b) du Décret du 1er Juillet 2020 et à l'Article 24.10 relatif à la cybersécurité, 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 révisée. Les serveurs de messagerie gouvernementale sont classifiés Niveau 2 (Sensible). L'infrastructure bare metal dédiée est recommandée — les solutions cloud public avec HSM dédié (y compris Microsoft Exchange Online avec Azure Dedicated HSM) sont acceptables.

Article 1 : Domaine et adresses officielles

Toute communication électronique officielle de l'administration publique haïtienne DOIT utiliser exclusivement le domaine .gouv.ht. L'utilisation d'adresses email personnelles ou de services grand public pour des communications officielles est formellement interdite.

Type d'utilisateur	Format d'adresse officielle
Ministre	prenom.nom@ministere.gouv.ht
Directeur Général	dg@institution.gouv.ht
Directeur technique	prenom.nom@institution.gouv.ht
Agent standard	prenom.nom@institution.gouv.ht
Alias institutionnel	info@institution.gouv.ht ou service@institution.gouv.ht

Article 2 : Solution de messagerie officielle requise

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

Article 3 : Spécifications techniques minimales

Paramètre	Exigence minimale	Remarques
Taille de boîte aux lettres	50 Go minimum par utilisateur	Illimitée pour Ministres et DG
Chiffrement en transit	TLS 1.3 — aucun fallback TLS 1.2	Art. 1.m (cybersécurité)
Chiffrement au repos	AES-256 avec clés BYOK/HSM exclusivement haïtiennes	Souveraineté des clés
MFA	Obligatoire pour TOUS les utilisateurs	Art. 24.10 — prévention usurpation
Rétention légale	5 ans min. — 10 ans documents financiers	Conformité légale haïtienne
Archivage in-place	Hold litige disponible	Investigation judiciaire
Anti-phishing	Filtrage natif + solution IHSI approuvée	Art. 24.10 (DIRC)
DMARC / DKIM / SPF	Configurables pour tous les domaines .gouv.ht	Authenticité des courriels officiels
Confidential Computing	Recommandé pour le traitement des emails	Protection Data in Use

Article 4 : Politique de contenu

Usages AUTORISÉS	Usages INTERDITS
Communications administratives et institutionnelles officielles	Campagnes politiques ou partisans
Notifications de services publics aux citoyens	Harcèlement, discrimination, contenu offensant
Coordination inter-institutionnelle (SyNSIP)	Spam, chaînes de lettres, messages viraux
Réponse aux demandes officielles des citoyens	Diffusion d'informations classifiées hors canaux sécurisés
Annonces internes non politiques	Activités commerciales ou personnelles

Article 5 : Rétention, archivage et cycle de vie

Type d'email	Durée de rétention	Méthode
Correspondance administrative courante	2 ans	Archive in-place — suppression automatique
Documents contractuels et financiers	10 ans	Archive avec hold — aucune suppression auto
Plaintes des citoyens	5 ans	Archive avec journalisation obligatoire
Communications CNSI / CONATEL	7 ans	Archive avec hold litige
Données classifiées ou sécurisées	Selon DIRC (Art. 24.10)	Canal sécurisé dédié

Article 6 : Garanties de souveraineté — Obligations contractuelles

Le prestataire retenu s'engage à :

- Ne pas divulguer les courriels gouvernementaux à toute autorité étrangère sans mandat haïtien
- Notifier l'IHSI dans les 48 heures de toute demande d'un gouvernement étranger
- Maintenir le BYOK/HSM haïtien actif en permanence — aucun accès aux clés sans autorisation IHSI
- Maintenir une infrastructure de redondance avec basculement automatique ≤ 1 heure

Article 7 : Sanctions

- Avertissement écrit (première infraction mineure)
- Suspension de l'accès à la messagerie officielle (répétition ou infraction grave)
- Sanction disciplinaire (règlement de la Fonction publique)

- Poursuites pénales pour cyberharcèlement, fraude ou violation de l'Article 29 du Décret

Article 8 : Calendrier de migration

Le plan de migration pilote de l'IHSI vers le service de messagerie souverain approuvé est décrit dans la Note de Service N° 001/IHSI/2026. Toutes les institutions du SyNSIP ont 18 mois après attribution du marché pour migrer l'intégralité de leur messagerie.

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