RÉPUBLIQUE D'HAÏTI

LIBERTÉ – ÉGALITÉ – FRATERNITÉ

Institut Haïtien de Statistique et d'Informatique (IHSI)

Dir. N° 002/IHSI/2026 | DIRECTIVE

NORMES TECHNIQUES — MATÉRIELS, LOGICIELS ET INFRASTRUCTURE CLOUD SOUVERAINE

Conformément à l'Article 24.13(b) du Décret du 1er Juillet 2020 mandatant la DNT de l'IHSI pour concevoir les normes techniques des institutions publiques, 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 présentes normes révisées. Elles intègrent la protection tricouche, la classification à 4 niveaux, l'acceptation des fournisseurs cloud publics avec BYOK/HSM dédié, et la redondance obligatoire.

Partie 1 : Normes matérielles — Postes de travail

Type d'appareil	Processeur	RAM	Stockage	OS	Réseau
Bureau (administration)	Intel Core i5 / AMD Ryzen 5 ou sup.	16 Go	256 Go SSD NVMe	Windows 11 LTSC / Ubuntu 22.04 LTS	Gigabit + Wi-Fi 6
Portable (terrain)	Intel Core i5 / AMD Ryzen 5	16 Go	256 Go SSD NVMe	Identique bureau	Gigabit + 4G/5G
Serveur (dérogation IHSI req.)	2x Intel Xeon Silver ou équivalent	64 Go+	RAID 10 (1 To+)	Rocky Linux 9 / Windows Server 2022	10 GbE

Partie 2 : Normes logicielles

Catégorie	Logiciels approuvés	Remarques
Systèmes d'exploitation	Windows 11 LTSC, Rocky Linux 9, Ubuntu 22.04 LTS	Mises à jour automatiques obligatoires
Bureautique	LibreOffice 7+, Microsoft Office 2021+ (si licence volume)	LibreOffice préféré pour maîtrise des coûts
Antivirus / EDR	Windows Defender for Endpoint ou équivalent certifié	Signatures MAJ toutes les 4 heures
Bases de données	PostgreSQL 15+, MariaDB 10.6+ ou équivalent open source	Sur infrastructure cloud approuvée

Navigateurs	Firefox ESR, Google Chrome (gestion centralisée IHSI)	Extensions approuvées IHSI seulement
Messagerie	Service souverain approuvé par l'IHSI — bare metal recommandé	Aucun serveur local — aucun service grand public

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	Bare metal dédié OBLIGATOIRE	OBLIGATOIRE HSM physique FIPS 140-2 Niv. 3 sous	OBLIGATOIRE Confidential Computing

	naissance) Données fiscales personnelles (DGI) Dossiers médicaux (MSPP) Données judiciaires (MJSP) Sécurité nationale et défense Données électorales (ONI) Clés cryptographiques de l'État	(serveur physique exclusif)	contrôle haïtien exclusif	(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.

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 PUBLIC SOUVERAIN	Cloud public mutualisé ISO 27001 obligatoire HSM DÉDIÉ chez fournisseur (physiquement inaccessible au fournisseur) BYOK — fournisseur sans accès aux clés Confidential Computing disponible Peut être soumis au CLOUD Act Clauses contractuelles notification 48h obligatoires	AWS (CloudHSM) Azure (Dedicated HSM) Google Cloud (EKM + Confidential VM)	Niveaux 2, 3, 4 (Niveau 1 avec Confidential Computing obligatoire)	AUTORISÉ sous conditions BYOK/HSM dédié
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

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

Partie 4 : Conformité et audit

Exigence	Fréquence	Responsable
Revue des certifications du prestataire	Annuelle	IHSI
Inventaire et revue des clés HSM	Trimestrielle	IHSI (DIRC)

Vérification configuration BYOK/HSM	Semestrielle	IHSI + prestataire
Test Confidential Computing (données Niveau 1)	Annuelle	IHSI + tiers approuvé
Test de basculement entre fournisseurs	Semestrielle	IHSI + prestataires
Test d'intrusion de l'infrastructure cloud	Semestrielle	IHSI + tiers approuvé
Audit de conformité du prestataire	Sur demande (72h préavis)	IHSI

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

[Prénom NOM]
Directeur Général de l'IHSI

Résolution CNSI N° XX/2026
Circulaire MEF N° XX/2026

[Prénom NOM]
Me Brunache — Conseiller juridique