REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
---
SERVICES DU PREMIER MINISTRE
---
SECRETARIAT GENERAL
---
PROGRAMME NATIONAL DE PREVENTION ET DE LUTTE CONTRE LES ZOONOSES EMERGENTES ET RE EMERGENTES
---
SECRETARIAT PERMANENT
---

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
---
PRIME MINISTER'S OFFICE
---
SECRETARIAT GENERAL
---
NATIONAL PROGRAM FOR THE PREVENTION AND FIGHT AGAINST EMERGING AND RE EMERGING ZOONOSES
---
PERMANENT SECRETARIAT
---

COHIS

# CADRE DE GOUVERNANCE DES DONNÉES ET SÉCURITÉ DES INFORMATIONS

## CAMEROON ONE HEALTH INFORMATION SYSTEM (COHIS)

**Septembre, 2025**

coopération allemande
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Organisation des Nations Unies pour l'alimentation et l'agriculture
Organisation mondiale de la Santé
Organisation mondiale de la santé animale

# TABLE DES MATIERES

# LISTE DES FIGURES



# LISTE DES TABLEAUX

# SIGLES ET ACRONYMES

| | | |
|---|---|---|
| **API** | : | *Application Programming Interface* |
| **CA** | : | *Certification Authority* |
| **CAHIS** | : | *Cameroon Animal Health Information System* |
| **CAMTEL** | : | *Cameroon Telecommunications* |
| **CDN** | : | *Content Delivery Network* |
| **CI/CD** | : | *Continuous Integration/Continuous Delivery* |
| **CID** | : | Confidentialité, Intégrité et Disponibilité |
| **CIM-11** | : | Classification Internationale des Maladies – 11e révision |
| **CNAQ** | : | Cadre National d'Assurance Qualité |
| **CRL** | : | *Certificate Revocation List* |
| **CT** | : | Comité Technique |
| **COHIS** | : | *Cameroon One Health Information System* |
| **DDoS** | : | *Distributed Denial-of-Service* |
| **DHO** | : | *Digital Health Office* |
| **DHIS2** | : | *District Health Information Software 2* |
| **FAO** | : | Organisation des Nations Unies pour l'Alimentation et l'Agriculture |
| **FHIR** | : | *Fast Healthcare Interoperability Resources* |
| **GIZ** | : | *Deutsche Gesellschaft für Internationale Zusammenarbeit* |
| **HL7** | : | *Health Level Seven International* |
| **HSM** | : | *Hard Security Module* |
| **IA** | : | Intelligence Artificielle |
| **ICD** | : | *International Classification of Diseases* |
| **INS** | : | Institut National de la Statistique |
| **ISO/IEC** | : | Organisation Internationale de Normalisation / Commission Electrotechnique Internationale |
| **IT** | : | *Information Technology* |
| **MTTD** | : | *Mean Time To Detect* |
| **MTTR** | : | *Mean Time To Recover* |
| **MFA** | : | *Multi-Factor Authentication* |
| **MINADER** | : | Ministère de l'Agriculture et du Développement Rural |
| **MINCOM** | : | Ministère de la Communication |
| **MINEPDED** | : | Ministère de l'Environnement, de la Protection de la Nature et du Développement Durable |
| **MINESUP** | : | Ministère de l'Enseignement Supérieur |
| **MINFOF** | : | Ministère des Forêts et de la Faune |
| **MINSANTE** | : | Ministère de la Santé Publique |
| **MINTOUL** | : | Ministère du Tourisme et des Loisirs |
| **MINEPIA** | : | Ministère de l'Élevage, des Pêches et des Industries Animales |
| **NAS** | : | *Network Attached Storage* |
| **OMS** | : | Organisation mondiale de la santé |

| | | |
|---|---|---|
| **OMSA** | : | Organisation mondiale de la santé animale |
| **OTP** | : | *One Time Password* |
| **OWASP** | : | *Open Worldwide Application Security Project* |
| **PCA** | : | Plan de Continuité d'Activité |
| **PKI** | : | *Public Key Infrastructure* |
| **PNPLZER** | : | Programme National de Prévention et de Lutte contre les Zoonoses Émergentes et Réémergentes |
| **PNUE** | : | Programme des Nations Unies pour l'environnement |
| **PRA** | : | Plan de Reprise d'Activité |
| **PRIDA** | : | Initiative politique et réglementaire pour l'Afrique numérique |
| **RAM** | : | *Random Access Memory* |
| **RBAC** | : | *Role-Based Access Control* |
| **RGPD** | : | Règlement Général sur la Protection des Données |
| **RPO** | : | *Recovery Point Objective* |
| **RSI** | : | Responsable de la Sécurité de l'Information |
| **RSSI** | : | Responsable de la Sécurité des Systèmes d'Information |
| **RTO** | : | *Recovery Time Objective* |
| **SBOM** | : | *Software Bill of Materials* |
| **SIEM** | : | *Security Information and Event Management* |
| **SMSI** | : | Système de Management de la Sécurité de l'Information |
| **SNIS** | : | Système National d'Information Sanitaire |
| **SNOMED CT** | : | *Systematized Nomenclature of Medicine – Clinical Terms* |
| **POS** | : | Procédure Opérationnelle Standard |
| **SORMAS** | : | *Surveillance, Outbreak Response Management and Analysis System* |
| **SQL** | : | *Structured Query Language* |
| **SSI** | : | Sécurité des Systèmes d'Information |
| **SSL/TLS** | : | *Secure Sockets Layer / Transport Layer Security* |
| **UA** | : | Union Africaine |
| **UIT** | : | Union Internationale des Télécommunications |
| **UE** | : | Union Européenne |
| **UNESCO** | : | Organisation des Nations Unies pour l'éducation, la science et la culture |
| **USAID** | : | *United States Agency for International Development* |
| **VM** | : | *Virtual Machine* |

# AVANT-PROPOS

Dans un monde de plus en plus interconnecté, les menaces sanitaires ne connaissent ni frontières ni disciplines. Les crises récentes, qu'elles soient d'origine animale, végétale, environnementale ou humaine, nous rappellent avec force que la santé humaine ne peut être pensée indépendamment de celle des animaux, des plantes et des écosystèmes. Le Cameroun, engagé dans la mise en œuvre de l'approche Une Seule Santé, entend renforcer sa capacité à anticiper, détecter et répondre efficacement aux menaces sanitaires émergentes et réémergentes, en s'appuyant sur une information intégrée, fiable et accessible.

C'est dans cet esprit que le *Cameroon One Health Information System* (COHIS) a été conçu : une plateforme innovante, interopérable, au service de la prévention, de la coordination et de la prise de décision éclairée. Son architecture repose sur la mutualisation des efforts, la valorisation des savoirs sectoriels et doit s'appuyer sur une gouvernance rigoureuse des données.

La gouvernance des données est le socle essentiel sur lequel repose l'ambition du Cameroun. Sans cadre de gestion clair, partagé et cohérent des données multisectorielles, aucun système d'information, aussi avancé soit-il, ne saurait répondre aux exigences de qualité, de sécurité et de réactivité qu'impose la santé publique contemporaine.

Le présent cadre de gouvernance vient formaliser les principes, rôles, règles et bonnes pratiques qui assureront la confiance, l'efficacité et la durabilité de cet outil stratégique. Élaboré de manière participative sous la coordination du Programme National de Prévention et de Lutte contre les Zoonoses Émergentes et Réémergentes (PNPLZER), avec le soutien de la Cellule Informatique du Ministère de la Santé Publique (MINSANTE) et de la *Deutsche Gesellschaft für Internationale Zusammenarbeit* (GIZ) à travers le projet *One Health Data Alliance Africa*, ce cadre reflète la volonté du Cameroun de se doter de standards élevés en matière de gestion de données, alignés sur les cadres internationaux tout en respectant les spécificités nationales.

Ce document est un appel à la coresponsabilité, responsabilité partagée entre tous les secteurs et acteurs détenteurs d'enjeux importants du mécanisme de collecte, analyse et partage des données de santé globale. Il s'adresse à tous les acteurs – producteurs, utilisateurs, régulateurs – des données de santé humaine, animale, végétale et environnementale, les invitant à adopter une culture commune de la donnée fondée sur l'éthique, la transparence, la sécurité et la qualité.

Nous espérons que ce cadre contribuera à faire du COHIS un véritable levier de souveraineté sanitaire, d'innovation, et de collaboration multisectorielle au service du bien-être des populations et de la résilience du système de santé camerounais.

# RESUME EXECUTIF

Le Manuel de Gouvernance des Données et de Sécurité des Informations de la plateforme *Cameroon One Health Information System* (COHIS) constitue un instrument stratégique visant à encadrer la gestion, l'utilisation et la protection des données multisectorielles mobilisées dans le cadre de l'approche Une Seule Santé au Cameroun.

Ce document a été élaboré dans un contexte marqué par la nécessité de renforcer la collaboration intersectorielle et de disposer de mécanismes fiables d'intégration, d'analyse et de partage des données pour anticiper et répondre efficacement aux menaces sanitaires à l'interface santé humaine – santé animale – santé végétale – santé environnementale.

Ses objectifs sont entre autres de :

- Définir les principes directeurs de gouvernance des données (transparence, sécurité, interopérabilité, redevabilité) ;
- Clarifier les rôles et responsabilités des parties prenantes dans la collecte, la validation, l'accès, le partage et l'utilisation des données ;
- Établir des protocoles standards pour l'échange sécurisé d'informations ;
- Promouvoir la protection des données sensibles et la conformité aux normes nationales et internationales soutenir la prise de décision fondée sur des données probantes pour la prévention, la préparation et la réponse aux risques sanitaires.

Le cadre de Gouvernance des Données et de Sécurité des Informations de la plateforme COHIS s'applique à l'ensemble des acteurs institutionnels, techniques et financiers engagés dans la plateforme COHIS. Il couvre les aspects liés à l'architecture de données, aux mécanismes de gestion de la qualité, à la cybersécurité, à la confidentialité et aux modalités d'interopérabilité avec d'autres systèmes nationaux et régionaux. Sa mise en œuvre repose sur une dynamique collaborative entre les ministères sectoriels, les agences spécialisées et les partenaires techniques, sous la coordination du Programme National de Prévention et de Lutte contre les Zoonoses Émergentes et Réémergentes (PNPLZER)/Plateforme *Une Seule Santé* du Cameroun.

Il est attendu de ce document de planification technique qu'il permette :

- Une meilleure fiabilité et disponibilité des données pour la surveillance et la planification sanitaire ;
- Une coordination renforcée entre les secteurs pour anticiper les épidémies et gérer les urgences de santé publique ;
- Une sécurisation accrue des flux d'information et une responsabilisation des acteurs.

Ce manuel pose les bases d'une gouvernance numérique solide, garantissant que la plateforme COHIS devienne non seulement un outil de collecte et d'analyse, mais également un levier stratégique de résilience sanitaire nationale et régionale. Sa réussite dépendra de l'appropriation collective, de la mise en application rigoureuse et de l'amélioration continue par tous les acteurs impliqués. Une contribution significative au rayonnement du Cameroun comme pays pionnier en Afrique dans l'opérationnalisation d'un système numérique intégré *Une Seule Santé*.

# COMITÉ TECHNIQUE DE RÉDACTION

## SUPERVISION

Pr. Séraphin Magloire FOUDA, Ministre, Secrétaire Général des Services du Premier Ministre, Président du Comité d'Orientation Stratégique (COS) de la Plateforme Une Seule Santé.

## COORDINATION

M. Sali Ballo, Chargé de Mission, Premier Ministère, Coordonnateur du Comité Technique (CT) ;

M. Sahadio Gilbert, SPM;

M. Ihong III, SPM;

Dr. Conrad Nkuo, Secrétaire Permanent, PNPLZER ;

Mme. Elisabeth Dibongue, Secrétaire Permanent Adjoint, PNPLZER ;

Dr. Garga Gonne, Directeur des Services Vétérinaires, MINEPIA, Coordonnateur Adjoint du CT ;

Dr. Esso Linda, Directeur de la Lutte contre la Maladie, les Épidémies et les Pandémies, MINSANTE, Membre du CT ;

Mme Maha Ngalie, Directeur de la Faune et des Aires Protégées, MINFOF ;

M. Adama Saidou, Conseiller Technique N°1, MINEPDED ;

Pr. Mofor Clautilde, Inspecteur des Services No 1, MINESUP, Membre du CT ;

Mme Ndzie Ntsama Angèle, Directeur de la Protection Civile, MINAT ;

Dr. Amina Djoulde Christelle, Directeur de la Coopération Scientifique et Technique, MINRESI ;

M. Oyebok Emmanuel Achaki, Directeur de la Promotion du Tourisme et des Loisirs, MINTOUL, Membre du CT ;

Dr. Nying Charles Shey, Direction de la Réglementation et du Contrôle de la Qualité des Intrants et des Produits Agricoles, MINADER ;

Mme Djeny Ngando Damaris, Chef de Cellule de Suivi, MINCOM, Membre du CT.

# ÉQUIPE DE RÉDACTION

M. Bakeneghe Batoum Guy, MINSANTE

M. Massom Eithel, MINSANTE

M. Nkomba Samuel, MINSANTE

M. Gwos Jean, MINSANTE

M. Mouangue Christian, MINSANTE

M. Mbamè Nkoutou, MINSANTE

Dr. Okiwah Abiambe Boris, MINEPIA

Dr. Ndongo Njiki Serge, MINEPIA

M. Atangana Kouna Joseph, MINEPDED

Mme Ekom Ange, MINFOF

M. Toki Mahap Maurice, MINFOF

Mme Daknou Lentcheu Irène Christiane, MINADER

M. Nguelo Colince, MINADER

M. Abondo Olivier, MINEPAT

M. Messina Yves Bertrand, MINEPAT

Mme Batomen Mbiakop Anne, MINRESI

M. Oba'a Bilo'o Etienne Patrick, MINEE

M. Eko Efoulou Edouard, MINEE

M. Mah Philippe Valdez, MINFI

Mme Nga Véronique, MINESUP

M. Eyem Georges Clément, INS

M. Takwa Habib Palay, ANTIC

M. Tchala Mboudou Thaddée, ANTIC

Mme Ebieline Hélène, ROOHCAM

Eloundou Nka Marc Cyrille, OMS

M. Murke Julius, GIZ

Mme Habiba Issa Muller, GIZ

Mme Bilack Rose Maeva, GIZ

M. Batalong Luc Yannick, GIZ

M. Pamoe Estebanc, GIZ

Dr. Fouogue Sonna Wilfred, PNPLZER

Dr. Ayissi Ayissi Gaspard PNPLZER

Dr. Njapdounke Pare Khadidja, PNPLZER

Mme Fokou Kuignou Lorraine, PNPLZER

Mme Benouke Ngosso Audrey, PNPLZER

M. Kuicheu Thierry Didier, PNPLZER

Dr. Cha-Ah Crystella Ngong, PNPLZER

Mme Ngo Mpan Berthe, PNPLZER

Dr. Aissatou Kodji Vandi, PNPLZER

Dr. Hanan El Oumar, PNPLZER

Dr. Amawota Alvine, PNPLZER

Dr. Jouegouo Fezeu Fride, PNPLZER

M. Khalil Sali, PNPLZER

Mme Tezempa Naomie, PNPLZER

M. Naga Fongang Stéphane, PNPLZER

Mme Azekeng Raissa, PNPLZER

Dr Nguimdjio Liliane, PNPLZER

Dr. Liz Pipi, PNPLZER

Mme Nouché Nadine, PNPLZER

M. Numvi Collins, PNPLZER

Mme Limnyuy Gladys, PNPLZER

Mme Che Lum Sidonie, PNPLZER

# REMERCIEMENTS

Le cadre de gouvernance des données et sécurité des informations du *Cameroun One Health Information System* (COHIS), est le résultat d'un processus enclenché depuis 2016, avec la mise en place du Programme Zoonoses et les travaux d'élaboration des procédures opérationnelles standardisées de partage des données entre les secteurs. Cet engagement des sectoriels se matérialise davantage en 2024 avec l'adoption du Plan d'Action Nationale *Une Seule Santé*.

COHIS est donc le fruit de la volonté politique du gouvernement camerounais à travers le Programme Zoonoses / Plateforme *Une Seule Santé,* et l'appui technique et financier des partenaires, notamment l'USAID, la GIZ-OHDAA, la FAO et l'OMS.

Nos remerciements vont à l'endroit de toutes les parties prenantes pour leur soutien inestimable, multiforme et leur contribution à la conception et au développement du COHIS, de même qu'à l'élaboration, la revue, la finalisation et l'adoption du présent cadre de gouvernance.

# CONTEXTE, OBJECTIFS ET PORTÉE

## Contexte et justification

Le contexte mondial de cette dernière décennie est marqué par l'émergence croissante de menaces sanitaires d'origine humaine, animale, végétale et environnementale. Pour y faire face, la nécessité et la pertinence d'une approche intégrée et collaborative de la santé telle que l'approche *Une Seule Santé* (*One Health*) ne fait plus débat. Cette approche, adoptée et recommandée par l'Organisation mondiale de la Santé (OMS), l'Organisation Mondiale de la Santé Animale (OMSA), l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO) et le Programme des Nations Unies pour l'environnement (PNUE), repose sur la reconnaissance que les santés humaine, animale, végétale et environnementale sont inextricablement liées et donc interdépendantes.

Le Cameroun, résolument engagé dans cette vision holistique édictée par le référentiel *Une Seule Santé*, a initié des actions innovantes en vue de mieux coordonner les réponses aux crises sanitaires, de prévenir les risques zoonotiques et de renforcer la résilience du système de santé dans son ensemble. C'est dans ce sens qu'une plateforme nationale intégrée de collecte, de traitement, de visualisation et d'analyse des données multisectorielles : le *Cameroon One Health Information System* (COHIS), a été pensée.

Développé sous la coordination du Programme National de Prévention et de Lutte contre les Zoonoses Émergentes et Réémergentes (PNPLZER), avec le soutien technique de la Cellule Informatique (CI) du Ministère de la Santé Publique (MINSANTE) et l'appui du projet One Health Data Alliance Africa mis en œuvre par la GIZ, COHIS est conçu comme une plateforme collaborative, reposant sur l'approche du data mesh. Cette architecture distribue les responsabilités de production, d'analyse et de valorisation des données aux différents secteurs tout en assurant la cohérence, la sécurité et la qualité des flux d'information via une plateforme partagée.

Aussi, pour garantir une utilisation efficace, éthique, sécurisée et durable de cette plateforme, il est impératif de mettre en place un cadre formel de gouvernance des données. Le présent document constitue ainsi un référentiel stratégique et opérationnel pour organiser, encadrer et piloter la gestion des données dans COHIS.

## Objectifs du cadre de gouvernance des données

L'objectif principal du cadre de gouvernance des données du COHIS est de permettre une collaboration fiable, transparente, légale et durable entre les secteurs partenaires de la plateforme *Une Seule Santé* tout en sécurisant l'information. Il vise à transformer les données en ressources stratégiques pour l'amélioration des mécanismes de gestion de la santé humaine, la santé animale, la santé végétale, la surveillance environnementale, la lutte contre les maladies zoonotiques et la prise de décisions éclairées. De façon spécifique, ce cadre poursuit les objectifs ci-après.

### 1 Planifier et organiser

Le cadre de gouvernance des données COHIS fournit une base structurée pour la planification stratégique et l'organisation opérationnelle des processus de données dans tous les secteurs et institutions impliqués. Il vise à garantir une circulation fluide et contrôlée de l'information, en réduisant les silos tout en clarifiant les responsabilités.

### 2 Promouvoir la transparence

Le cadre promeut la transparence et la traçabilité sur l'ensemble du cycle de vie des données. Il définit clairement les rôles et responsabilités en matière de production, de propriété, de contrôle d'accès, de gestion éthique et de supervision des données. Il établit des mécanismes de journalisation, de restriction d'accès, de partage conditionnel, tout en s'assurant que les producteurs conservent un droit de regard sur l'utilisation des données qu'ils fournissent.

### 3 Gérer les risques

En tant que dispositif préventif, le cadre structure des outils pour identifier, évaluer et atténuer les risques liés aux données, incluant les cyber-menaces, la perte d'information, la non-conformité ou la défaillance des systèmes. Il introduit des protocoles d'évaluation régulière, de réponse aux incidents, de sauvegarde, et de continuité des opérations, essentiels dans un contexte multisectoriel à haut niveau d'interdépendance.

### 4 S'aligner aux lois et règlements

Le cadre veille à l'alignement des pratiques de gouvernance des données COHIS sur les lois nationales et les standards internationaux relatifs à la protection des données, à la cybersécurité, aux droits numériques et à l'éthique.

### 5 Faciliter la maintenance et la durabilité

Conscient que la gouvernance des données est un processus évolutif, le cadre prévoit des dispositions pour la pérennité du système.

### 6 Promouvoir la qualité des données

Enfin, le cadre met un accent particulier sur la qualité des données, pierre angulaire de toute analyse ou politique fiable.

## Portée et périmètre

Le présent cadre s'applique à toutes les données et métadonnées intégrées dans la plateforme COHIS, qu'elles soient produites, collectées, partagées, stockées ou analysées dans le cadre des activités de santé humaine, animale, végétale et environnementale.

Par ailleurs, ce cadre s'adresse à un large éventail d'acteurs concernés par la gestion et l'exploitation des données dans le cadre de l'approche *Une Seule Santé*, à savoir : les administrations sectorielles, les producteurs de données, les analystes, les utilisateurs, les administrateurs techniques et les partenaires techniques et financiers.

## Ancrage stratégique

Le cadre de gouvernance des données et de sécurité des informations de la plateforme COHIS s'inscrit en parfaite cohérence avec les priorités et orientations stratégiques du Cameroun dans les secteurs de la santé publique, de la santé animale, de la santé végétale et de la protection de l'environnement.

L'ancrage stratégique du cadre de gouvernance de COHIS se traduit par son alignement avec les grandes orientations de la Stratégie Nationale de Développement 2020-2030, qui met l'accent sur la bonne gouvernance, le capital humain et la résilience. En renforçant la production et le partage de données multisectorielles, COHIS contribue à la mise en œuvre de la Stratégie Sectorielle de la Santé, notamment en matière de couverture sanitaire universelle et de gestion des urgences. Son ancrage dépasse le champ de la santé humaine pour intégrer les priorités des Stratégie Nationale de Santé Animale et Vétérinaire, les politiques agricoles et de sécurité alimentaire, ainsi que les stratégies environnementales et climatiques.

Enfin, il s'inscrit dans la vision nationale de transformation numérique et de cybersécurité, garantissant une gouvernance des données conforme aux standards internationaux. Ainsi, ce dispositif confère une cohérence d'ensemble aux interventions sectorielles et matérialise l'approche *Une Seule Santé* comme levier de la sécurité sanitaire et du développement durable du Cameroun.

# CHAPITRE 1 : PRINCIPES DE GOUVERNANCE

Les principes de gouvernance des données et de sécurisation des informations sont basés sur les lois, règlements et règles qui régissent la collecte, le traitement, le stockage et le partage des données d'une part, la sécurité et la qualité des données d'autre part. Ainsi, la gouvernance des données dans le cadre du système COHIS s'inspire des normes internationales, conventions régionales et sous-régionales et se conforme aux lois nationales en vigueur au Cameroun. Par conséquent, ce cadre de gouvernance s'appuie sur les principes ci-après.

## 1.1. Conformité

La conformité vise à assurer l'alignement et l'harmonisation du système COHIS avec les réglementations nationales et les normes internationales en matière de protection des données. Les normes et lois suivantes sont applicables :

### 1.1.1. Normes et stratégies nationales et internationales

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la

sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;

- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;
- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité ;
- Stratégie Sectorielle de la Santé 2020-2030 : élaborée pour la première fois en 2001, elle définit le cadre d'orientation de l'action gouvernementale en matière de santé, avec un accent mis pour cette édition actualisée, sur les problèmes d'intersectorialité en matière de santé.

### 1.1.2. Lois et actes du Cameroun

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

### 1.1.3. Autres textes réglementaires :

- Décret n° 2021/690 du 02 Décembre 2021 fixant les modalités d'application de la loi n°·2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun ;

- Circulaire n° 003/CAB/PM du 28 Mars 2018 : elle établit les règles spécifiques à la gestion des documents et données confidentiels dans l'administration publique, notamment via l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC).

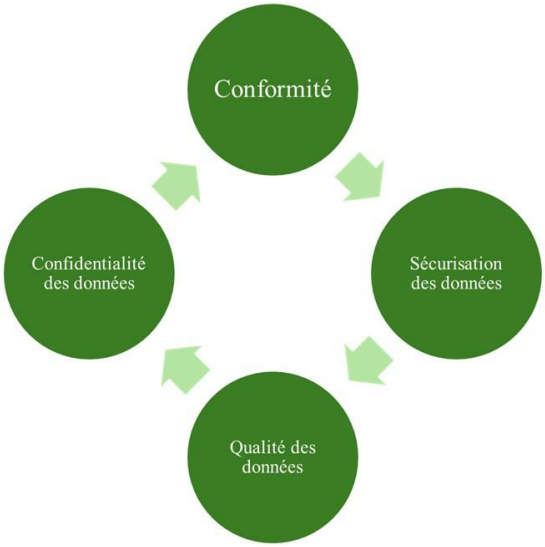


**Figure 1 : Principes de gouvernance**

## 1.2. Sécurité des données

Dans le cadre du fonctionnement de la plateforme nationale d'intégration des données multisectorielles *One Health* du Cameroun dénommée COHIS, il est institué un ensemble de mesures visant à garantir la sécurité, la confidentialité, l'intégrité, la disponibilité et la traçabilité des données collectées, stockées, transformées et diffusées par ledit système d'information.

À cet effet, il est mis en œuvre des mesures de sécurité techniques, organisationnelles et procédurales, fondées sur une analyse des risques liés à la nature des données traitées, à leur niveau de sensibilité, à leur finalité, ainsi qu'à leur origine sectorielle (santé humaine, santé animale, santé végétale, santé environnementale, etc.).

Les mesures de sécurité appliquées s'appuient sur des standards internationalement reconnus, en particulier les normes ISO/IEC 27001 (Système de management de la sécurité de l'information), ISO/IEC 27002 (Code de bonnes pratiques pour la sécurité de l'information) et ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information), et s'inscrivent dans une logique de conformité, de prévention et de responsabilité partagée entre les parties prenantes.

A ce titre, sont notamment appliqués :

- La gestion des accès basée sur les rôles et responsabilités fonctionnelles, assortie de mécanismes d'authentification renforcée ;

- Le chiffrement obligatoire des données sensibles, tant lors de leur transit que pendant leur stockage, afin d'assurer leur protection contre toute forme d'interception, d'altération ou de divulgation non autorisée ;
- La mise en place de journaux (logs) pour la traçabilité des accès, des modifications et des extractions de données, régulièrement audités ;
- La sécurisation des infrastructures logicielles et matérielles via des dispositifs de pare-feu, de surveillance réseau, de détection d'intrusion et d'analyse des vulnérabilités ;
- La réalisation régulière d'audits de sécurité de l'information, internes et par des tiers indépendants, en vue de garantir la conformité continue aux exigences de sécurité ;
- La sauvegarde des données de haute disponibilité (annexe 9) ;
- La sensibilisation des utilisateurs aux bonnes pratiques des mesures de sécurité ;
- La mise en œuvre d'un processus structuré de gestion des risques conformément à la norme ISO/IEC 27005, incluant l'identification et la classification des actifs informationnels, l'analyse des menaces et vulnérabilités, l'évaluation de la criticité des risques, le traitement adapté (réduction, évitement, transfert ou acceptation), ainsi que le suivi et la révision périodique du registre des risques.

Les mesures de sécurité adoptées sont révisées périodiquement, notamment à la suite des audits susmentionnés ou en cas d'évolution contextuelle (apparition de nouvelles menaces, modification des flux de données, changement de périmètre réglementaire). En outre, les dispositifs de sécurité sont proportionnés au niveau de risque de perte, de compromission ou de fuite de données, évalué sur la base d'une cartographie des données traitées par la plateforme. L'ensemble des mesures de sécurité actuellement en vigueur dans le cadre de l'exploitation du système COHIS fait partie intégrante de ce cadre de gouvernance.

## 1.3. Qualité des données

Dans un contexte où la plateforme intègre des données issues de multiples sources, la qualité des données constitue un pilier fondamental de la gouvernance de l'information. En effet, les décisions stratégiques, les analyses scientifiques, la détection précoce des alertes sanitaires et l'évaluation des politiques publiques dépendent directement de la fiabilité, la pertinence et l'utilité des données collectées, partagées et croisées. Par conséquent, la qualité des données et la gestion des métadonnées jouent un rôle important, et des processus doivent être mis en place pour garantir que tous les produits de données et ensembles de données respectent les normes minimales de qualité des données et de gestion des métadonnées. Les approches de gestion de la qualité des données s'inspirent des standards ISO 8000, ISO/IEC 11179 et s'alignent au Cadre National d'Assurance Qualité (CNAQ). Les dispositifs mis en place pour garantir la qualité des données sont les suivants :

#### 1.3.1. Cadre de qualité partagé multisectoriel

- Définition conjointe, entre secteurs, des normes de qualité applicables à chaque type de donnée ;
- Adoption de standards sectoriels et internationaux.

#### 1.3.2. Référentiel des règles de validation

- Mise en œuvre de règles automatiques pour détecter les erreurs ou incohérences (validation à l'ingestion, contrôle en aval) ;
- Mise à disposition de guides de saisie ou d'échange de données pour les producteurs.

#### 1.3.3. Outils de contrôle qualité intégrés à la plateforme

- Tableaux de bord qualité (taux d'erreurs, complétude, fréquence de mise à jour, …) ;
- Alertes automatiques en cas de données manquantes, incorrectes ou suspectes.

#### 1.3.4. Rétroaction aux sources de données

- Signalement systématique des anomalies détectées aux fournisseurs ;
- Mécanismes collaboratifs de correction ou de mise à jour.

#### 1.3.5. Formation et responsabilisation des acteurs

- Sensibilisation des producteurs de données aux enjeux de qualité ;
- Attribution claire de rôles (Intendant des données etc.) pour chaque secteur.

#### 1.3.6. Évaluation périodique de la qualité

- Audits réguliers des jeux de données critiques ;
- Rapports de qualité partagés lors des comités techniques intersectoriels.

### 1.4. Confidentialité et protection des données personnelles

Pour garantir la confidentialité des informations sensibles dans les secteurs de la santé humaine, animale, végétale et environnementale, le COHIS doit fonctionner avec des processus robustes pour protéger les données. Seul le personnel autorisé peut consulter ou traiter ces données, et des mesures techniques et organisationnelles robustes doivent être mises en place pour les protéger contre la divulgation non autorisée, la falsification ou la perte. En effet, un élément clé de la gouvernance des données est la classification et la protection des données en fonction de leur niveau de confidentialité. Pour s'assurer que les données sont traitées de manière appropriée, toutes les informations, qu'elles proviennent de sources de santé humaine, animale, végétale ou environnementale, doivent être systématiquement classifiées en fonction de leur sensibilité.

Au niveau le plus élémentaire, les données se répartissent en quatre catégories :

- Les données publiques, telles que les rapports agrégés ou les tendances épidémiologiques générales, ne présentent aucun risque si elles sont divulguées et ne nécessitent donc pas de restrictions spécifiques ;
- Les données internes, y compris les procédures opérationnelles ou les analyses internes, doivent être protégées par des contrôles d'accès et une surveillance du système afin d'éviter toute utilisation abusive interne non autorisée ;
- Les données confidentielles, telles que les chiffres de surveillance au niveau de l'établissement ou les résultats de laboratoire, nécessitent des mesures de protection plus strictes, notamment des restrictions d'accès basées sur les rôles et le cryptage ;
- Les données personnelles ou sensibles (noms, des numéros d'identification nationaux, des dossiers médicaux détaillés, données d'exploitation agro-sylvo-pastorale, données financières, etc.) exigent le plus haut niveau de protection. Cela inclut le cryptage avancé, la pseudonymisation ou l'anonymisation, et le respect des normes juridiques et éthiques.

Pour respecter cela, la classification des données doit se faire au niveau des produits de données et au niveau des éléments de données individuels. Un catalogue de données centralisé ou un registre de métadonnées doit maintenir l'état de la classification et les procédures de traitement requises pour les types de données standard. En raison de la nature particulièrement sensible des données personnelles, qu'elles soient liées à des humains, à des animaux ou des végétaux, des procédures spéciales doivent être suivies pour protéger ces informations. En effet, toutes données personnelles ne peuvent être téléchargées sur le COHIS qu'après l'autorisation explicite d'un Intendant des données désigné. Ce processus d'approbation garantit que le traitement des données est justifié et documenté de manière appropriée. Toute demande de téléchargement doit inclure une description claire de la finalité de l'utilisation, du niveau de classification des données attribué et une justification de la raison pour laquelle les données sont nécessaires à la fin prévue.

Ensuite, lorsque cela est techniquement et opérationnellement possible, les données doivent être cryptées ou dépersonnalisées, par des techniques de pseudonymisation ou d'anonymisation. L'accès à toutes les données qui restent identifiables doit être régi par des politiques de contrôle d'accès différentiel, garantissant que seul le personnel autorisé peut voir ou traiter ces informations.

Enfin, le principe d'auditabilité et de traçabilité assure la responsabilisation dans le traitement des données. Chaque accès ou transfert de données doit être enregistré dans une piste d'audit sécurisée et infalsifiable. Cela permet d'effectuer des examens rétrospectifs, de détecter les anomalies ou les violations et de se conformer aux exigences légales et institutionnelles.

# CHAPITRE 2 : ROLES ET RESPONSABILITES

Dans toute initiative touchant à la gestion de données ou à la sécurité des systèmes d'information, la clarté des rôles et responsabilités est non seulement souhaitable, mais absolument essentielle. Une définition précise des fonctions de chacun est le fondement sur lequel repose l'efficacité opérationnelle, la responsabilisation et la réussite globale. D'où l'importance cruciale d'établir et de communiquer clairement qui fait quoi, qui est responsable de quoi, et quelles sont les attentes envers chaque acteur impliqué. En effet, une allocation rigoureuse des rôles et des responsabilités permet de minimiser les chevauchements, d'optimiser les flux de travail, de renforcer la collaboration interministérielle, d'assurer une gouvernance solide et une gestion proactive des défis. La gouvernance des données dans le cadre du COHIS est pilotée par le Comité d'Orientation Stratégique du PNPLZER. Ledit comité désigne les acteurs opérationnels. Les principaux rôles des acteurs du COHIS s'inscrivent globalement dans l'une des quatre catégories suivantes : Développement, Coordination et Supervision ; Facilitation et Gestion ; Productions de données, consommation de données (figure 2).

## 2.1. Développement, Coordination et Supervision

Ces acteurs sont responsables de définir l'orientation stratégique, d'assurer l'alignement avec les objectifs organisationnels, et de superviser la mise en œuvre des politiques de gouvernance des données. Il s'agit des entités ci-après indiquées.

- Le **Comité d'Orientation Stratégique du PNPLZER** : il assure la gouvernance globale et l'orientation stratégique de la plateforme COHIS.
- **Secrétariat Permanent du PNPLZER** : il dirige le développement et l'exécution de la stratégie de gouvernance des données du COHIS, assurant son alignement avec les objectifs organisationnels plus large. Il lui est attribué entre autres responsabilités :
    - La coordination des processus de traitement des données ;
    - La conformation du système aux normes de qualité de données nationaux et internationaux (ISO 8000) ainsi qu'au respect des processus relatifs aux données ;
    - L'élaboration des plans de gestion des données ;
    - La définition des normes de présentation des données, applicables à la plateforme *One Health* ;
    - La gestion conjointe avec la Cellule Informatique du MINSANTE des comptes utilisateurs ;
    - La gestion de l'environnement de partage de données ;
    - L'élaboration d'un plan de renforcement de capacités pour l'utilisation du COHIS ;
    - La veille informationnelle au profit du *One Health* ;
    - La promotion de l'outil COHIS et de son rôle dans la prise de décision sur la base des données multisectorielles ;

- Le suivi/évaluation.

Les détails des termes de référence du PNPLZER figurent à l'annexe 15.

- **Cellule Informatique du MINSANTE** : il lui est attribuée entre autres responsabilités :
  - La gestion de la sécurité des données de la plateforme COHIS ;
  - La conformation du système aux standards de sécurité nationaux et internationaux (ISO 270001, 270002 et 270005) ;
  - La conformation aux normes et réglementations applicables ;
  - La documentation des procédures de sécurité ;
  - L'élaboration de la politique de sécurité de la plateforme COHIS ;
  - La définition des procédures de sauvegarde des incidents, de sauvegardes et des plans de reprise d'activité ;
  - L'hébergement de la plateforme COHIS et l'administration du serveur de la plateforme ;
  - La veille sécuritaire pour la migration vers de nouvelles solutions ;
  - La gestion conjointe avec le PNPLZER des comptes utilisateurs ;
  - La sensibilisation de tous les acteurs aux bonnes pratiques de sécurité.

  Les détails des termes de référence de la Cellule Informatique du MINSANTE figurent à l'annexe 16.

## 2.2. Facilitation et Gestion

Il s'agit de la gestion quotidienne des données, s'assurant que les données soient correctement traitées, stockées, partagées et utilisées de manière systématique, éthique et responsable. Les acteurs en charge sont responsables de la conservation à long terme des données et des documents, en veillant à ce que les archives historiques et les ensembles de données critiques soient stockés en toute sécurité, accessibles et correctement maintenus pour une utilisation future.

Il s'agit d'individus ou de groupes d'individus ou d'entités, notamment :

- **Staff technique du PNPLZER (Intendants de données)** : il est chargé de gérer et maintenir la qualité ainsi que l'accès et la réutilisation responsables des données. Il lui est attribué entre autres responsabilités :
  - L'exécution du plan de gestion des données : il gère l'ensemble des informations contenues dans le système ;
  - La mise en application des normes de présentation des données ;
  - L'appui aux producteurs et aux consommateurs de données afin de garantir des données fiables, sécurisées et conformes aux normes de qualité ;

- L'exécution du plan de formation.

- **Staff technique de la Cellule Informatique du MINSANTE (Intendants de données)** : il est chargé de gérer et maintenir la sécurité ainsi que l'accès aux données. Il lui est attribué entre autres responsabilités :

  - L'exécution du plan de sécurisation des données ;
  - La mise en application des normes de sécurisation et protection des données ;
  - L'appui aux producteurs et aux consommateurs de données afin de garantir des données sécurisées et conformes aux normes de confidentialité ;
  - La co-exécution du plan de formation ;
  - La veille technologique.

## 2.3. Production de données

Les **Points Focaux COHIS** sont chargés d'appliquer les principes généraux de traitement et de sécurisation des données de leurs secteurs. Ils collaborent avec les staffs techniques du PNPLZER et de la Cellule Informatique du MINSANTE pour garantir la qualité des données introduite dans la plateforme. Il leur est attribué entre autres responsabilités :

- L'alimentation de la plateforme en données, la production des analyses et des rapports : pour générer des tableaux de bord, des rapports d'activité, des analyses de tendances ou des études spécifiques ;
- La gestion de la qualité et de la sécurité des données dans leurs domaines d'activité ;
- La définition des règles d'accès aux données sectoriels pour les utilisateurs de COHIS ;
- La description des métadonnées sectorielles, afin qu'elles soient compréhensibles par les utilisateurs COHIS ;
- La participation à l'innovation : en explorant et en combinant les données de différentes manières, ils peuvent découvrir de nouvelles corrélations, générer des hypothèses et stimuler l'innovation.

## 2.4. Consommation de données

Les **consommateurs de données** sont les utilisateurs finaux de la plateforme, qui exploitent les données mises à leur disposition pour diverses finalités. En effet ils :

- Utilisent les données pour la prise de décision : qu'il s'agisse de décisions opérationnelles, tactiques ou stratégiques, les consommateurs de données transforment les informations brutes ou traitées en insights actionnables ;
- Contribuent à l'amélioration de la qualité des données : par leur utilisation quotidienne, ils peuvent identifier des anomalies, des incohérences ou des lacunes dans les données, remontant ces informations aux intendants de données.

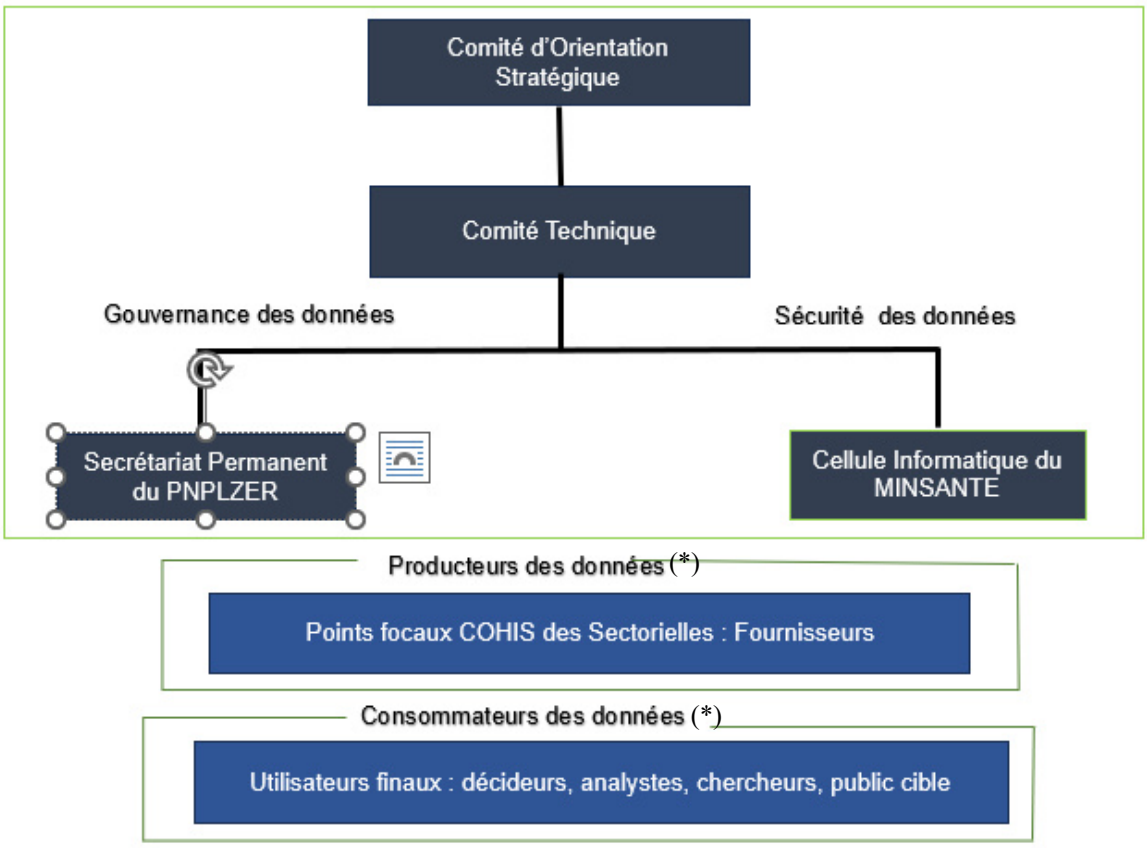


**Figure 2 : Organigramme**

(*) Liste non exhaustive des producteurs et consommateurs de données : MINEPIA, MINSANTE, MINEPDED, MINFOF, MINADER, MINEE, MINEPAT, ROOHCAM, etc.

# CHAPITRE 3 : PROCESSUS DE GESTION DES DONNÉES

Les données sont un atout fondamental pour la plateforme COHIS, servant de base à la prise de décision, à l'innovation et à l'optimisation des performances de notre système de santé. Toutefois, leur valeur ne peut être pleinement exploitée sans une gestion rigoureuse et structurée, qui englobe l'ensemble des étapes de leur cycle de vie, de la collecte au traitement, en passant par le stockage et la sécurisation. Ce chapitre présente le processus de gestion des données à mettre en œuvre afin de garantir la qualité, l'intégrité, la sécurité et la disponibilité des informations. Nous explorerons les différentes phases de ce cycle de vie des données, de leur collecte initiale à leur archivage ou suppression, en passant par leur stockage, leur traitement, leur sécurisation et leur mise à disposition.

## 3.1. Processus de gestion des produits données

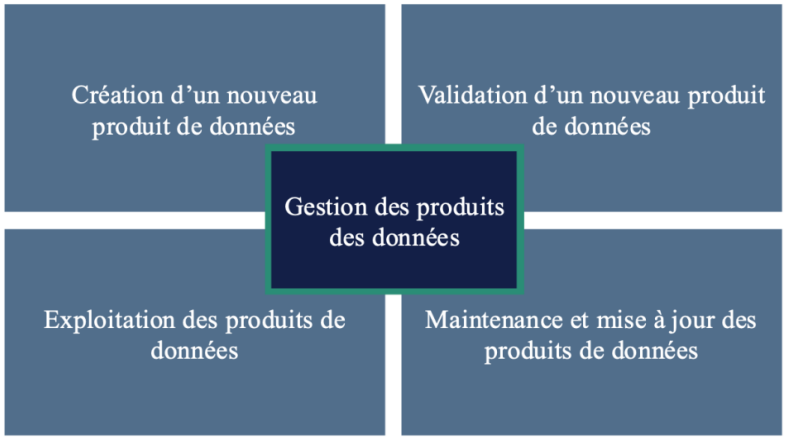


**Figure 3 : Processus de gestions des données.**

Le principe du self-service sur lequel repose la plateforme COHIS exige la mise en œuvre de processus de gestion des données. Deux acteurs majeurs interviennent dans le processus de gestion de données : les producteurs de données (point focaux COHIS sectoriels) et les intendants de données. Alors que les producteurs sont autonomes dans la prise d'initiative de création de nouveaux produits de données, les intendants de données doivent superviser le processus et s'assurer que les normes de protection des données, de qualité et de gestion des métadonnées ont été respectées lors de la création et de l'utilisation d'un nouveau produit de données. Dans la plateforme COHIS, les producteurs de données et les intendants de données travaillent ensemble sur quatre processus :

- Création d'un nouveau produit de données ;
- Validation d'un nouveau produit de données ;
- Maintenance et mise à jour des produits de données ;
- Exploitation des produits de données.

### 3.1.1. Création d'un nouveau produit de données

Les producteurs de données sont responsables de la création de nouveaux produits de données. Les intendants ont pour rôle de soutenir les producteurs de données dans le processus. Il les consulte, s'assure de la conformité du processus aux normes de sécurité et de qualité des données. C'est de la responsabilité des producteurs de données d'informer les intendants ainsi que le responsable de la gouvernance des données de la création d'un nouveau produit de données. Les producteurs de données définissent l'accès aux éléments de leur produit de

données pour les autres utilisateurs après avis de l'intendant. La bonne pratique de création d'un nouveau produit de données recherchée s'articule autour des points suivants :

- Les producteurs de données définissent et valident un cas d'utilisation avec leur hiérarchie ;
- Les producteurs décrivent le jeu de données pour le cas d'utilisation avec l'appui de l'intendant de données (voir annexe 6) ;
- Les intendants informent le responsable de la gouvernance des données pour avis de non-objection, et facilitent la création du produit de données (conception du pipeline de données et de la chaîne de processus).

Techniquement, la création du produit de données implique les étapes décrites ci-après.

#### *3.1.1.1.Collecte des données*

Le producteur de données doit proposer des bonnes pratiques pour la collecte des données au sein de son institution. Le principe général veut que la plateforme COHIS ne collecte pas les données à leur source. Au lieu de cela, les producteurs de données mettent en place un pipeline de données vers leurs propres sources de données. Par conséquent, le processus visant à garantir la qualité des données et à se conformer aux lois et réglementations nationales en matière de collecte de données incombe au producteur de données. Néanmoins, les intendants doivent veiller à ce que les producteurs de données des différents secteurs respectent les politiques et procédures établies dans ce cadre de gouvernance des données. Il s'agit d'une part de règles visant à garantir la sécurité des données et d'autre part de règles visant à garantir la qualité des données (voir « processus de gestion de la qualité des données »).

#### *3.1.1.2.Nettoyage/traitement des données*

Le producteur de données, conjointement avec l'intendant des données, doit mettre en place des procédures pour identifier et corriger les données incorrectes, incomplètes ou dupliquées. Cela se fera autant que possible au moyen d'outils automatisés pour le nettoyage des données. Au cours du processus de nettoyage et de traitement des données, il est essentiel que les producteurs de données gèrent les métadonnées en toute éthique. Les producteurs de données sont tenus de se conformer à des normes de métadonnées convenues, telles que les normes pour les noms de lieux ou les codes pour les maladies (exemple : CIM-11). Les producteurs de données doivent donc consulter un intendant de données pour appliquer les transformations de données nécessaires.

#### *3.1.1.3.Stockage des données*

L'intendant des données conjointement avec le responsable de la gouvernance de données doit utiliser des structures de stockage sécurisées et optimisées pour l'accès et l'analyse des données. Il doit assurer une gestion efficace des métadonnées pour faciliter la recherche et la récupération des données. A date, la plateforme COHIS stocke les données dans sa base de données conformément aux pipelines de données configurés et met à jour ces données selon la fréquence définie dans les chaînes de processus.

### 3.1.2. Validation d'un nouveau produit de données

Les intendants de données sont responsables de la validation des nouveaux produits de données. Le responsable de la gouvernance des données veille à ce que tous les nouveaux produits de données aient été validés par l'intendant de données, conformément à la norme ISO 8000 portant sur la qualité des données. Il s'agit entre autres :

- Respect des lois et règles en matière de protection des données, en particulier si les données comprennent des informations personnellement identifiables ;
- Respect des normes de métadonnées (annexe 2) ;
- Description du produit de données selon le modèle prédéfini (annexe 6) ;
- Configuration avec le producteur de données des indicateurs automatiques de contrôle de la qualité des données pour le produit de données ;
- Assurance de la compréhensibilité de la description des éléments du produit de données afin de permettre une traçabilité des données appropriée et l'exhaustivité des données pour les autres utilisateurs ;
- Établissement des règles d'accès aux produits de données : le producteur de données définit les droits d'accès en concertation avec l'intendant de données (annexe 6).

L'intendant de données communiquera les droits d'accès au responsable de la gouvernance des données, qui les mettra en œuvre.

### 3.1.3. Maintenance des produits de données

Les produits de données existants doivent être maintenus et feront probablement l'objet de mises à jour régulières. La maintenance des produits de données est analogue à leur création, sous la responsabilité conjointe des producteurs de données et des intendants de données.

- Maintenance préventive : les intendants de données doivent examiner régulièrement les produits de données existants pour garantir la conformité aux normes de protection et de qualité des données. Ils doivent produire un rapport d'évaluation semestriel des produits de données existants ;
- Maintenance corrective : en cas de changements mineurs ou de bug, les producteurs de données doivent notifier les intendants de données et mettre à jour la fiche de description des données (annexe 6). En cas de maintenance palliative envisagée, mûrir la démarche afin d'aboutir à un correctif durable ;
- Maintenance évolutive : en cas de changements majeurs (modification de la structure du produit de données, etc.), les producteurs de données doivent, avec les intendants de données développer une nouvelle instance de la fiche de description des données (annexe 6).

Le responsable de la gouvernance des données doit maintenir un registre des produits des données avec description des métadonnées ainsi que la description de leurs droits d'accès.

### 3.1.4. Exploitation des produits de données

Une fois les produits de données disponibles, ils peuvent faire l'objet d'exploitations variées par les producteurs et consommateurs de données à la limite des restrictions d'accès préétablies. Plusieurs cas de figures sont possibles comme ci-après indiqué.

#### *3.1.4.1.Consultation du catalogue de produits de données*

Le catalogue renferme la liste des produits de données, y compris les métadonnées rattachées. Après consultation, les producteurs, autre que le propriétaire, peuvent demander l'accès total ou partiel (éléments) à un produit de données. L'autorisation d'accès à ce produit de données relève de la responsabilité du producteur propriétaire du produit de données en question.

#### *3.1.4.2.Analyse des données*

L'analyse des données se fera principalement via le module Superset du COHIS et sera de la responsabilité des producteurs de données. Néanmoins, pour des analyses plus complexes, les producteurs de données peuvent faire appel aux intendants de données, si l'analyse des données nécessite par exemple des méthodes ou techniques avancées.

#### *3.1.4.3.Visualisation des données*

La visualisation des données est l'un des principaux objectifs de la plupart des produits de données et c'est généralement le résultat que la plupart des consommateurs de données utiliseront. Pour chaque cas d'utilisation à implémenter à partir d'un produit de données, le producteur doit renseigner et garder à jour la fiche de description des données (annexe 6).

## 3.2. Processus de gestion de la qualité des données

La gestion de la qualité des données dans la plateforme COHIS comme dans tout autre système numérique est cruciale, elle permet de réduire les erreurs d'analyse et de faciliter l'interopérabilité entre systèmes afin de prendre les bonnes décisions. Le responsable de la gouvernance des données est chargé de veiller au respect des normes de qualité des données. En effet, chaque produit de données doit respecter les normes de qualité des données établies (annexe 2). Ces normes suivent les standards ISO 8000 et ISO/IEC 11179 qui énoncent les exigences minimales relatives aux dimensions de la qualité des données, telles que l'exhaustivité, l'actualité, la cohérence interne, la cohérence externe et l'exactitude. De plus, ces normes décrivent les exigences relatives à la conformité aux normes de métadonnées telles que la CIM-11 ou les codes de localisation.

Afin d'assurer la conformité aux normes de métadonnées et aussi permettre aux utilisateurs de comprendre les données venant des différents producteurs des données, à chaque produit des données est jointe une fiche de description des données (annexe 6) et les formats des métadonnées sont définis dans un registre des métadonnées/dictionnaire des données (annexe 7). Notons que la plateforme COHIS génère un catalogue de produits actualisés en

permanence, et les intendants de données sont chargés de la mise en œuvre opérationnelle de l'application des normes qui régissent la qualité des données de la plateforme COHIS.


**Figure 4 : Normes de qualité des données.**

### 3.2.1. Cadre normatif de qualité des données

Les principales normes qui régissent la qualité des données dans la cadre de la plateforme COHIS sont les suivantes : a) La norme ISO/IEC 11179 - portant sur la métadonnée. Elle s'intéresse à comment décrire les données pour qu'elles soient comprises, trouvées et réutilisées de manière cohérente. b) La norme ISO 8000 - portant sur la qualité de la donnée. Elle s'intéresse à la qualité et l'intégrité des données échangées ou gérées.

#### *3.2.1.1. La norme ISO/IEC 11179 : portant sur la métadonnée*

La norme ISO/IEC 11179 est une norme internationale qui encadre la manière dont les métadonnées doivent être décrites, organisées et gérées dans un système d'information. Elle vise à assurer que les données échangées ou analysées dans des contextes différents gardent le même sens. Elle ne se limite pas à lister des noms de données, mais elle impose une structuration rigoureuse de la manière dont chaque élément de donnée est défini, nommé, versionné, catégorisé, et validé. Le cœur de cette norme est de garantir l'interopérabilité sémantique, c'est-à-dire le fait que les systèmes ne partagent pas uniquement des chiffres, mais qu'ils partagent aussi la signification de ces chiffres.

Dans le contexte du COHIS cette norme permet de répondre au besoin fondamental d'aligner les données issues de secteurs différents – santé humaine, santé animale, environnement – pour une surveillance intégrée des risques sanitaires. Les systèmes sources tels que DHIS2 pour la santé humaine ou CAHIS pour la santé animale utilisent des formats, des vocabulaires, et des structures différentes. Le registre de métadonnées basé sur ISO/IEC 11179 agit ici comme une colonne vertébrale conceptuelle commune qui permet de centraliser la définition des indicateurs et des éléments de données clés, tout en rendant leur signification partageable et interopérable.

Concrètement, cela signifie que chaque élément de donnée utilisé dans la plateforme COHIS – par exemple "nombre de cas suspects de rage animale" – est défini de manière unique, avec une définition complète, une source validée, une version bien identifiée, et des valeurs attendues clairement spécifiées. Cela permet d'éviter qu'un même indicateur ne soit interprété différemment selon les ministères ou les plateformes. Chaque élément de donnée enregistré suit un cycle de vie précis : il peut être proposé, validé, approuvé, modifié ou retiré. Ce processus est encadré par des data stewards. Ce sont eux qui formulent ou valident les définitions, documentent les modifications, s'assurent que les producteurs de données utilisent bien les éléments enregistrés dans le registre.

Cette norme modélise la donnée en une architecture en trois couches :

- Conceptuelle : définit les idées abstraites derrière les données (ex. "sexe d'une personne") ;
- Logique : décrit comment ces idées sont représentées comme éléments de données ;
- Physique : gère les formats, types, codes utilisés dans les bases de données.

Ses principales composantes sont représentées dans le tableau ci-dessous avec exemples :

**Tableau 1 : Composants de la norme ISO/IEC 11179.**

| Composante | Définition technique | Exemple : Sexe du patient |
|---|---|---|
| **Concept de donnée** | Idée abstraite représentant une unité de signification en contexte. | "Sexe biologique du patient" |
| **Domaine conceptuel** | Ensemble de valeurs conceptuelles possibles pour une donnée. | {Masculin, Féminin, non connu} |
| **Champ de valeurs** | Ensemble défini de valeurs permises, avec format et représentation technique. | {1 = Masculin, 2 = Féminin, 9 = Inconnu} (codé sous forme numérique) |
| **Concept d'élément de données** | Association d'un concept de donnée à une classe d'objet (entité concernée). | "Sexe de la personne" = (Concept : sexe, Objet : personne) |
| **Classe d'objet** | Ensemble d'objets réels ou abstraits auxquels les données se rapportent. | Personne |
| **Élément de donnée** | Implémentation concrète d'un élément de données Concept avec une valeur de domaine spécifique. | "Sexe_du_patient" (codé 1, 2, 9) |
| **Terme de représentation** | Mot utilisé pour refléter la forme des données dans les noms (selon convention de nommage) | "Sexe" est le terme représentatif dans "Sexe_du_patient" |
| **Nom de l'élément de données** | Libellé officiel et standardisé d'un élément de donnée. | "Sexe_du_patient" |
| **Enregistrement** | Processus d'enregistrement formel dans un registre de métadonnées validé. | "Sexe_du_patient" enregistré dans le registre national de métadonnées santé |
| **Situation administrative** | Statut du cycle de vie d'un élément (soumis, validé, publié, retiré…). | Validé |

#### *3.2.1.2.La norme ISO 8000 : portant sur la qualité des données*

Cette norme propose une liste de critères d'évaluation à partir desquels il est possible d'attribuer une note numérique sur une certaine échelle afin de jauger la qualité des données de notre système.

Le tableau ci-dessous propose les critères (dimensions), une illustration des problèmes abordés et les améliorations proposées.

**Tableau 2 : Critères d'évaluation de la norme ISO 8000.**

| Dimension | Problème | Amélioration ISO 8000 | Exemple |
|---|---|---|---|
| **Exactitude** | Valeurs aberrantes (150 m3 vs 15 m3) | Validation automatique des seuils | Rejet des valeurs hors plage réaliste |
| **Complétude** | Mois ou régions manquants | Vérification de champs obligatoires | Alerte si une région n'a pas de données |
| **Cohérence** | Unités et formats variés | Harmonisation des formats et unités | Tout exprimé en mm, dates au format AAAA-MM-JJ |
| **Actualité** | Données livrées trop tard | Délais normalisés de soumission | Livrer les données dans les 5 jours suivant le mois |
| **Accessibilité** | Fichiers dispersés | Centralisation et contrôle d'accès | Données stockées dans un entrepôt partagé |
| **Traçabilité** | Source des données inconnue | Ajout de métadonnées (source, date, version) | Chaque ligne indique le capteur et la date de réception |
| **Compréhensibilité** | Abréviations locales incompréhensibles | Dictionnaire de données partagé | "PRCP" remplacé par "Précipitation mensuelle (mm)" |
| **Réutilisabilité** | Incompatibilité avec d'autres systèmes | Format structuré et standardisé | Intégration directe dans les outils de prévision agricole |

### 3.2.2. Processus de gestion de la qualité des données

Le processus de gestion de la qualité des données dans le cadre du COHIS comprend une série d'activités et procédures mises en œuvre de manière systématique pour garantir que les données répondent aux exigences définies en termes de précision, complétude, cohérence, actualité, pertinence et intégrité. Les principales étapes de ce processus sont les suivantes :

#### *3.2.2.1.Définition et modélisation des données*

Cette étape vise la création (et/ou la mise à jour) d'un référentiel clair, structuré de partage des données utilisées dans le système.

*i) Activités principales*

- Identifier les entités métier (ex.: patient, cas de maladie, fournisseur, produit, commune, etc.) ;

- Décomposer ces entités en éléments de données unitaires (ex.: nom, code, sexe, statut) ;
- Définir chaque élément selon la structure ISO/IEC 11179 :
  - Nom de l'élément ;
  - Définition formelle ;
  - Type de représentation (code, texte, nombre, booléen…) ;
  - Format standard (ex : AAAA-MM-JJ pour une date) ;
  - Valeurs autorisées (domaines de valeurs ou nomenclatures).

ii) *Livrable*

Modèle de données conforme avec le Dictionnaire de données / registre de métadonnées (annexe 7).

#### *3.2.2.2.Profilage des données et mesure de la qualité des données*

Cette étape vise à analyser les données existantes pour en identifier les défauts avant toute décision ou utilisation analytique. Elle consiste à évaluer les données à travers des dimensions de qualité standardisées selon la norme ISO 8000 (Annexe 2). Les dimensions clés inclus (tableau 3).

**Tableau 3 : Critères d'évaluation de la norme ISO 8000 pour un User case.**

| Dimension clés | Description | Exemple |
|---|---|---|
| **Exactitude** | Donnée conforme à la réalité | Un nom correctement orthographié |
| **Complétude** | Donnée présente quand attendue | Aucun champ vide pour "sexe" |
| **Cohérence** | Données non contradictoires entre elles | Sexe = "M" et Civilité ≠ "Madame" |
| **Actualité** | Donnée à jour par rapport au temps réel | Statut du patient mis à jour |
| **Accessibilité** | Donnée disponible pour les bons utilisateurs | Pas de restriction indue |
| **Unicité** | Données non redondantes | Pas de doublon d'identifiants |

*i) Activités principales*

- Exploration des bases de données pour :
  - Détecter les valeurs manquantes ;
  - Identifier les doublons ;
  - Repérer les incohérences de formats ;
  - Vérifier les règles métiers (ex.: date de naissance < date actuelle).
- Détection des anomalies statistiques (valeurs aberrantes) ;
- Calcul des dimensions de qualité des données.

ii) *Livrable*

Document d'évaluation de la qualité des données.

### *3.2.2.3.Nettoyage / Amélioration*

C'est une étape a pour objectif de corriger ou atténuer les erreurs identifiées lors des étapes précédentes.

*i) Méthodes*

- Normalisation : homogénéiser les formats (ex : "Femme", "fem", "F" → "F") ;
- Validation automatique : règles de validation (registre, domaines de valeurs, …) ;
- Suppression / fusion de doublons ;
- Remplissage guidé ou semi-automatique des valeurs manquantes ;
- Correction manuelle des erreurs critiques.

ii) *Livrables*

- Liste des données corrigées ;
- Journal des modifications.

### *3.2.2.4.Documentation, auditabilité et traçabilité*

Il s'agit ici de garantir que chaque donnée peut être comprise, retracée et auditée à tout moment.

*i) Activités principales*

- Versionnage des métadonnées (en insérant la date de dernière édition et le nom de l'éditeur dans le nom du fichier) ;
- Journalisation des modifications (logs) ;
- Documentation des sources de données ;
- Preuves de conformité aux normes (rapports, audits).

*ii) Livrables*

Documentation technique et fonctionnelle : fiche de description des données (annexe 6) et mise à jour du dictionnaire de données/registre des métadonnées (annexe 7) si besoin.

### *3.2.2.5.Gouvernance et contrôle qualité continue*

Afin d'assurer une amélioration continue de la qualité et une responsabilité claire autour des données, il est primordial de mettre en place une gouvernance et un contrôle de la qualité des données en continue dans le COHIS. Ses composants clés sont :

*i) Rôles et responsabilités*

- Producteur de données : propriétaire métier de la donnée ;
- Intendant de données : gardien de la qualité et conformité ;

- Gouvernance de données : responsable technique du stockage.

*ii) Politiques et procédures*

- Règles de nommage ;
- Cycle de vie des données ;
- Gestion des accès.

*iii) Livrables*

Promptitude de validation des livrables, résultats de l'évaluation de la qualité des données, liste des données corrigées, descriptions des jeux de données, registres des métadonnées.

*3.2.2.6.Interopérabilité et réutilisation*

Elle vise à permettre que les données soient partageables et utilisables dans d'autres systèmes (interopérabilité sémantique).

*i) Actions*

- Réutilisation d'éléments de données standardisés ;
- Publication de définitions dans un registre partagé.

*ii) Livrables*

- Fiches de métadonnées exportables (annexe 7) ;
- Catalogue des données interopérables.

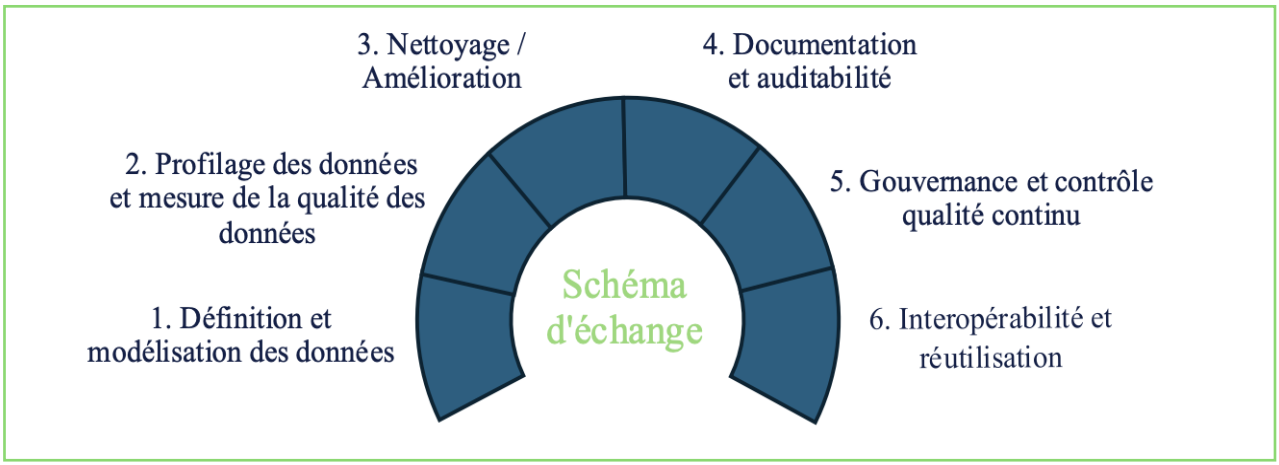


**Figure 5 : Schéma d'échange**

# CHAPITRE 4 : ACCES ET SECURITE

Les données étant le moteur du système COHIS, leur sécurité et leur accessibilité contrôlée sont des impératifs absolus. Bien plus qu'une simple contrainte technique, la protection des informations sensibles et la garantie d'un accès adéquat sont au cœur de la confiance entre les acteurs et représentent le socle de la pérennité des activités. Ce chapitre abordera en profondeur les piliers fondamentaux de cette démarche allant de la sécurité et la protection des données face aux menaces internes et externes, à l'importance cruciale de la sauvegarde pour assurer la continuité des opérations et la résilience du COHIS face aux imprévus. Nous développerons les principes, les stratégies et les bonnes pratiques permettant de bâtir une infrastructure de données robustes, où l'intégrité, la confidentialité et la disponibilité des informations sont assurées, transformant ainsi les défis de sécurité en opportunités de confiance et de performance :

- **Confidentialité :** protéger l'accès non autorisé aux informations sensibles stockées ou transitant via l'infrastructure ;
- **Intégrité :** garantir que les données ne sont pas altérées de manière non autorisée et qu'elles sont fiables ;
- **Disponibilité :** assurer que les systèmes et les données sont accessibles aux utilisateurs légitimes quand ils en ont besoin.

## 4.1. Sécurisation / protection

La sécurité de l'information est un élément crucial pour garantir la confiance, la cohérence et la disponibilité des données, mais surtout s'assurer que les données sensibles ne puissent pas tomber entre les mains de personnes non autorisées. Le responsable de la gouvernance des données sera chargé de définir et de s'assurer du respect des mesures de sécurité de l'information. Le processus de la sécurisation de l'information sera assuré par des mesures techniques et opérationnelles. Les mesures techniques visant la protection contre les accès non autorisés aux données à travers des méthodes d'authentification, de détection et de la prévention des intrusions. Les mesures opérationnelles comprennent des approches visant à la sensibilisation des utilisateurs sur les aspects de sécurité des données et la responsabilisation des utilisateurs pour la gestion des données conformément aux normes établies suivant les orientations des normes ISO/IEC 27001 :2022. A cet effet les mesures retenues dans le présent cadre inclus les volets suivants :


**Figure 6 : Mesures de sécurité.**

## 4.2. Contrôles organisationnels

Les contrôles organisationnels visent l'établissement d'une gouvernance garantissant que la sécurité est intégrée dans les processus de gouvernance et les opérations sur la plateforme. Ce cadre de gouvernance des données est un élément crucial pour définir les principes de la gestion de la sécurité de l'information, tels que la définition des rôles et des responsabilités des acteurs abordés dans son Chapitre 2 et des procédures de gestion de la sécurité de l'information. Les principales procédures de gestions de la sécurité de l'information définis sont :

### 4.2.1. Le cadre de gestion de risques

Il a pour objectif l'identification, l'évaluation, la gestion et la surveillance des risques de sécurité qui pourraient avoir une incidence sur la confidentialité, l'intégrité et la disponibilité de la plateforme COHIS. Il établit une approche structurée pour s'assurer que tous les ministères et intervenants participants peuvent accéder aux données et les partager en toute sécurité, tout en minimisant les menaces potentielles de cyber-attaques, d'utilisation abusive ou de défaillances opérationnelles. Le cadre favorise la confiance et le respect des normes nationales et internationales de protection des données, et de se fait une collaboration multisectorielle durable (annexe 8).

### 4.2.2. La politique de gestion des comptes

Elle définit les règles et procédures encadrant l'authentification des utilisateurs à travers la création, l'attribution, la modification, la suspension et la suppression des comptes utilisateurs ayant accès à la plateforme. Elle a pour objectif de :

- Empêcher tout accès non autorisé aux données ;
- Garantir que chaque compte est justifié, traçable et maîtrisé ;
- Réduire la surface d'attaque en éliminant les comptes dormants ou obsolètes ;
- Assurer la traçabilité complète des activités des utilisateurs.

L'ensemble des procédures y afférentes sont décrites dans l'annexe 10.

### 4.2.3. La réalisation des audits

La réalisation des audits réguliers du COHIS permet d'évaluer la conformité avec les politiques de gouvernance de données et d'identifier les domaines nécessitant des améliorations. Le responsable de la gouvernance des données est chargé de réaliser un audit annuel de la gouvernance des données, incluant un rapport sur la qualité des données et la sécurité de l'information. Les résultats de cet audit aident à vérifier que les politiques, procédures et mesures de sécurité définies sont correctement appliquées, efficaces et conformes aux exigences internes et externes (ex. ISO/IEC 27001, lois nationales). Quatre types d'audits sont à envisager notamment :

- **Audit technique :** analyse des configurations des systèmes, réseaux, infrastructures, vulnérabilités, tests d'intrusion. **Responsable :** consultant externe ; **Périodicité :** tous les 12 mois ;

- **Audit organisationnel :** évaluation des politiques, responsabilités, gouvernance, sensibilisation et coordination ministérielle. **Responsable :** Cellule Informatique du MINSANTE ; **Périodicité :** tous les 12 mois ;
- **Audit de conformité :** vérification des lois camerounaises et des directives UA. **Responsable :** Cellule Informatique du MINSANTE ; **Périodicité :** tous les 12 mois ;
- **Audit croisé interministériel :** réalisé entre les différents ministères pour favoriser la transparence et l'alignement des pratiques. **Responsable :** Responsable de la Sécurité des Systèmes d'Information sectoriel ; **Périodicité :** tous les 24 mois.

### 4.3. Contrôles des personnes

La gestion des facteurs humains est primordiale pour la sécurité des systèmes d'information. En effet, même avec des infrastructures techniquement robustes, l'erreur ou la mauvaise utilisation par les utilisateurs demeure la principale source de risque. C'est pourquoi le contrôle des personnes vise, dans un premier temps, à sensibiliser les utilisateurs à la sécurité. Il implique la mise en place des :

- Procédures d'intégration des utilisateurs (incluant l'obligation de comprendre et de signer une note de confidentialité des données) ;
- Processus rigoureux de gestion des utilisateurs et des accès ;
- Mesures de formation et de sensibilisation continues pour s'assurer que les utilisateurs maîtrisent les principes de protection des données et de sécurité de l'information.

La formation et la sensibilisation continues sont importantes pour permettre aux producteurs de données d'exploiter la valeur de leurs données et d'assurer la conformité aux normes de gouvernance des données. De plus, étant donné que les utilisateurs se connectent avec leurs propres appareils, le contrôle de ces derniers doit être géré par des politiques et des procédures relevant du contrôle des personnes. La liste actuelle des contrôles des personnes applicables dans la cadre du COHIS figure à l'annexe 11.

### 4.4. Contrôles physiques

La sécurisation des fondations de son infrastructure est un pilier essentiel de la sécurité des informations. Cela consiste à mettre en place des mesures de protection robustes dès les couches les plus basses et les plus critiques du système d'information. L'approche repose sur les principes suivants :

- **Réduire la Surface d'Attaque :** en sécurisant les éléments fondamentaux (réseaux, serveurs, systèmes d'exploitation, bases de données, hyperviseurs, firmware), on minimise les points d'entrée potentiels pour les attaquants, rendant plus difficile l'exploitation des vulnérabilités ;
- **Établir une Base de Confiance :** une infrastructure sécurisée sert de fondation solide sur laquelle repose la confiance de l'ensemble du système d'information. Si les couches de base sont compromises, toutes les couches supérieures (applications, données) sont également en danger ;

- **Prévenir les Compromissions Majeures :** les attaquants ciblent souvent les fondations pour obtenir un contrôle persistant et étendu sur le réseau. Sécuriser ces éléments permet de déjouer ces tentatives et d'empêcher des compromissions généralisées ;
- **Soutenir la Résilience et la Continuité des Activités :** une infrastructure résiliente, conçue avec la sécurité en tête, est mieux à même de résister aux attaques et aux pannes, assurant ainsi la continuité des services.

Il est à noter que les serveurs hébergeant le COHIS sont situés dans les infrastructures de CAMTEL (*Cameroon Telecommunications*), l'opérateur public historique du Cameroun. Conformément au contrat d'hébergement, CAMTEL est ainsi responsable de la sécurisation physique de ces infrastructures et donc de celle du COHIS en adéquation avec les principes susmentionnés. Rappelons que l'opérateur dispos d'un Datacenter Certifié Tier III attestant d'un niveau élevé de disponibilité, de sécurité, et de résilience, grâce à des redondances pour l'alimentation électrique, le refroidissement et le réseau, assurant un fonctionnement quasi continu de l'infrastructure.

## 4.5. Contrôles technologiques

Afin de renforcer la sécurité et d'automatiser les processus, les contrôles technologiques sont essentiels pour sécuriser une plateforme d'intégration de données. L'objectif principal est de renforcer et d'automatiser la sécurité des systèmes, en plaçant les contrôles technologiques au cœur de la protection de la plateforme d'intégration de données.

Cette sécurisation repose sur plusieurs piliers :

- **Authentification et autorisation :** mettre en place des mécanismes robustes pour garantir l'identité des utilisateurs et contrôler strictement leurs accès ;
- **Sécurité réseau :** assurer la protection du réseau à l'aide de pare-feu ;
- **Chiffrement des données :**
  - Chiffrer les communications via TLS ;
  - Sécuriser les informations sensibles pendant leur stockage, en appliquant des standards de chiffrement fiables.
  - Établir un cadre de journalisation et de surveillance robuste ;
  - Déployer un SIEM (Security Information and Event Management) pour la détection des intrusions et la surveillance des points d'extrémité (endpoints).

La liste actuelle des mesures techniques et opérationnelles figure à l'annexe 1.

## 4.6. Surveillance et gestion des incidents

Dans un environnement numérique d'intégration en continue de données tel que celui du COHIS, la simple mise en place de mesures de sécurité ne suffit pas à garantir une protection infaillible. La capacité à surveiller activement le système et à réagir efficacement face aux incidents est un pilier fondamental de sa résilience et de sa posture de sécurité. Il est donc d'une importance vitale de mettre en place des systèmes de surveillance continue pour détecter les

anomalies et les menaces potentielles, ainsi que les stratégies et les processus essentiels à une gestion d'incidents rapide et coordonnée en temps réel.

Il est de la responsabilité des responsables de la gouvernance des données de surveiller en permanence le respect des normes de gouvernance des données et de réagir à toute cyber-attaque ou violation de la conformité. En cas d'incident majeur, lesdits responsables sont chargés de remettre un rapport ad hoc au comité de gouvernance des données. Son action est appuyée par les intendants de données qui doivent signaler toute violation de la conformité aux normes de gouvernance des données des utilisateurs au responsable de la gouvernance des données.

Pour les détails du système de surveillance et gestion des incidents veuillez (voir annexe 14).

# CHAPITRE 5 : CADRE DE RENFORCEMENT DES CAPACITÉS

Dans un contexte où les exigences en matière de gouvernance des données évoluent rapidement notamment en raison des avancées technologiques, des impératifs de cyber sécurité et du besoin constant en personnel qualifié, il est crucial de mettre en place des mécanismes robustes, systématiques et durables de renforcement des capacités. La formation continue et la sensibilisation ciblée constituent les leviers clés pour assurer la pérennisation et l'efficience de la plateforme COHIS. Le renforcement des capacités repose sur 4 axes de compétences fondamentaux (figure 5) à développer :

- **Culture des données** : capacité à comprendre, interpréter, analyser et communiquer avec les données de manière critique et éclairée ;
- **Éducation aux données** : compréhension stratégique des données pour soutenir une prise de décision fondée sur des preuves par les décideurs ;
- **Accès aux données** : savoir manipuler, interroger et exploiter les données disponibles via la plateforme COHIS ;
- **Outils de données** : maîtrise des outils et fonctionnalités opérationnelles de la plateforme COHIS.

## 5.1. Objectifs

Le cadre de renforcement de capacité de la plateforme COHIS est structuré autour des objectifs fondamentaux suivants :

- Constituer et maintenir un pool d'experts qualifiés, prêts à répondre aux exigences du système ;
- Comprendre la valeur stratégique des données dans la prise de décision et l'amélioration des performances de toutes les sectorielles ;
- Maîtriser les normes, les référentiels et les bonnes pratiques en matière de gouvernance des données, notamment les standards ISO 27001, ISO 8000 et ISO 38505, qui exigent des compétences techniques et organisationnelles spécifiques ;
- Réduire les risques liés à la non-conformité et à la mauvaise gestion des données ;
- Favoriser une appropriation effective du cadre de gouvernance de la plateforme COHIS par tous les utilisateurs ;
- Faciliter une adaptation continue aux évolutions technologiques et fonctionnelles de l'outil.

## 5.2. Programme de formation

Le véritable moteur de performance du COHIS réside dans les compétences et l'adaptabilité des acteurs qui l'utilisent, le gèrent et l'optimisent au quotidien. La formation est donc un pilier indispensable à l'adoption, l'efficacité et la pérennité du système. Plusieurs programmes annuels de formation devront être développés et mis en œuvre pour renforcer les capacités des acteurs à travers les formations suivantes :

- Formation des administrateurs système et personnels IT (travaillant dans la technologie de l'information) de chaque sectorielle : développement de formations spécialisées à destination des équipes techniques pour assurer la maintenance, le soutien technique et l'évolution du système. Les administrateurs et personnels IT sectoriels bénéficieront d'une formation couvrant l'architecture technique du COHIS, la gestion des serveurs et des bases de données, les mécanismes de sauvegarde et de restauration, ainsi que le redéploiement du système en cas de panne ou de montée en charge. Des modules pratiques aborderont le suivi des performances, la gestion des fichiers de logs (journaux), la mise en œuvre de scripts d'automatisation, des outils sur le monitoring continu et des mesures de sécurité informatique nécessaires au bon fonctionnement du système ;
- **Formation à l'utilisation fonctionnelle de COHIS :**
  - La formation des intendants de données est conçue pour renforcer leurs compétences dans la gestion avancée des données. Elle inclut des sessions approfondies sur les processus d'extraction, de transformation et de chargement (ETL) ; l'évaluation de la qualité des données et le nettoyage ; l'utilisation de catalogues de métadonnées, et les pratiques de gouvernance (traçabilité, politiques d'accès, documentation). Une introduction aux techniques d'analyse augmentée par l'intelligence artificielle est également prévue avec des cas pratiques de prédiction, de classification et de détection d'anomalies avec un accompagnement technique mensuel pendant trois (03) mois pour l'implémentation des acquis sur le terrain ;
  - La formation des utilisateurs du niveau central se concentre sur l'exploitation opérationnelle du système. Elle couvre l'accès aux données, la production d'indicateurs, la transformation des jeux de données via des outils comme Apache Hop, et la création de tableaux de bord interactifs avec des outils de visualisation tel qu'Apache Superset®. Les participants apprendront à concevoir des produits de données répondant aux besoins des programmes sectoriels avec une session pratique finale de présentation de projets de données ;
- **Formations et activités pour améliorer l'utilisation des données produites par COHIS :**
  - La première activité est la formation sur les cas d'usage avancés, destinée aux intendants de données, aux utilisateurs centraux spécialisés, et aux consultants en science de données. Elle permettra de développer des modèles analytiques (par exemple, la prédiction des épidémies zoonotiques ou l'identification de foyers de vulnérabilité) à l'aide de bibliothèques Python, R, ou autres. Des ateliers pratiques permettront de concevoir des rapports dynamiques à valeur ajoutée. Cette formation sera organisée sous forme d'ateliers avec encadrement personnalisé ;

- La seconde activité est la tenue de réunions trimestrielles de revue des données, qui réuniront les points focaux multisectoriels. Ces rencontres auront pour objectif de valider collectivement les principales tendances épidémiologiques, les alertes en émergence, les lacunes en matière de données, et les recommandations d'action. Chaque réunion donnera lieu à la production d'un bulletin trimestriel *One Health*, réalisé en collaboration avec les institutions sectorielles ;
- Un modèle standard de bulletin sera développé. Il comprendra une structure harmonisée (résumé analytique, indicateurs clés, infographies, recommandations, …) permettant une diffusion cohérente des informations entre les différents niveaux d'intervention.

- **Formation sur la gouvernance des données et à la sécurité de l'information :** une formation régulière sera organisée pour les utilisateurs du niveau central. Elle portera sur les notions fondamentales de qualité des données, les exigences en matière de protection des données personnelles, la gestion des accès et les bonnes pratiques en cybersécurité. Cette activité vise à consolider la conformité du COHIS aux standards nationaux et internationaux de gestion sécurisée de l'information ;
- **Formalisation d'une politique de gestion des compétences critiques :** mise en place d'un cadre structuré de gestion et de transfert de savoir-faire garantissant une autonomie progressive des équipes et la pérennité des expertises nécessaires au fonctionnement optimal du COHIS.

### 5.3. Sensibilisation

Le bon fonctionnement de la plateforme COHIS dépend non seulement des capacités techniques des utilisateurs, mais aussi de leur conscience des risques liés à une mauvaise manipulation des données, et de leur adhésion aux principes de gouvernance. La sensibilisation vise à informer, mobiliser et responsabiliser tous les acteurs impliqués dans le traitement, la circulation et l'utilisation des données dans une logique de transparence, de conformité et de protection.

Le plan de sensibilisation poursuit les objectifs suivants :

- Promouvoir une compréhension partagée des principes de gouvernance des données ;
- Sensibiliser aux risques liés à la manipulation non sécurisée ou non éthique des données ;
- Renforcer l'adhésion aux politiques nationales et sectorielles de sécurité de l'information et de protection des données ;
- Encourager une gestion proactive des droits d'accès, du partage et de la confidentialité ;
- Créer un environnement de confiance autour de l'utilisation des données multisectorielles dans le cadre *One Health.*

Le plan de sensibilisation se base sur trois composantes :

- La première composante consiste en l'élaboration d'un guide utilisateur simplifié sur la gouvernance des données, des infographies explicatives, des cas de mauvaise gestion ou de bonnes pratiques, et des messages clés adaptés aux différents profils utilisateurs.
- La deuxième composante repose sur l'organisation de sessions de sensibilisation. Celles-ci seront intégrées dans les ateliers de formation. Les sessions seront participatives, avec des mises en situation (jeux de rôle, quiz, études de cas, …) pour renforcer la compréhension des principes de confidentialité, d'intégrité des données, d'accès différencié selon les rôles, et de gestion des incidents de sécurité.
- La troisième composante prévoit une campagne de communication continue. Elle utilisera les canaux internes (emails, groupes WhatsApp professionnels, …) pour diffuser chaque trimestre un message court ou une « bonne pratique du mois ». Cette campagne permettra de maintenir l'attention des utilisateurs sur les risques et les responsabilités liés aux données.

Ce plan de sensibilisation pourra être contextualisé au besoin selon l'urgence du pays, ou des difficultés rencontrées par les différents sectoriels.

# CHAPITRE 6 : CADRE DE SUIVI & ÉVALUATION

Dans tout projet, programme ou système complexe, la simple mise en œuvre des activités planifiées n'en garantit pas le succès. Dès lors, pour s'assurer que les objectifs seront atteints, que les ressources seront utilisées avec efficience et que les impacts souhaités se concrétisent, des mécanismes rigoureux de suivi et d'évaluation sont indispensables. Le mécanisme de suivi-évaluation (S&E) de la plateforme COHIS est un instrument essentiel pour garantir son efficacité opérationnelle, favoriser son adoption par les utilisateurs et maximiser son impact sur la prise de décision en santé publique. Le présent cadre conceptuel du suivi-évaluation du COHIS décrit les indicateurs clés de performance, les outils de collecte de données et les responsabilités des divers acteurs impliqués dans ce processus continu. Il servira de base au développement du plan global de suivi des activités de déploiement de la plateforme.

## 6.1 Objectifs du suivi-évaluation

Le cadre de suivi-évaluation de la plateforme COHIS est structuré autour des trois (03) objectifs fondamentaux suivants :

- **Efficacité technique** : mesurer la performance intrinsèque des fonctionnalités de la plateforme incluant les pipelines de traitement de données et les tableaux de bord. Il s'agit d'assurer que les processus techniques opèrent avec la fluidité et la fiabilité requises ;
- **Utilisation** : évaluer l'adoption effective de la plateforme par les secteurs cibles à savoir : la santé humaine, animale, végétale et environnementale. Cet objectif vise à comprendre l'engagement des utilisateurs et l'intégration du COHIS dans leurs pratiques quotidiennes ;
- **Évaluation** : il s'agit d'évaluer la contribution du COHIS aux décisions stratégiques et à la gestion des urgences épidémiologiques. Il est question de démontrer la valeur ajoutée concrète de la plateforme dans l'amélioration des résultats en santé humaine, animale, végétale et environnementale.

## 6.2 Indicateurs clés de performance

Les indicateurs de performance sont catégorisés pour une évaluation holistique de la plateforme, offrant une vision complète de ses performances et de son utilité :

**Tableau 4 : Indicateurs clés de performance.**

| Catégorie | Indicateurs | Niveau de référence |
|---|---|---|
| **Efficacité technique** | Taux de disponibilité de la plateforme (%) | ≥ 90 % |
| | Temps moyen pour charger les tableaux de bord | ≤ 2 minutes |
| | Pourcentage de jeux de données avec description des données | ≥ 95 % |
| **Utilisation** | Nombre d'utilisateurs actifs par rôle | ≥ au nombre de comptes créés |
| | Pourcentage des utilisateurs satisfaits | ≥ 85 % |

| | | |
|---|---|---|
| | Nombre des tableaux de bord configurés | ≥ au nombre de sectorielles impliquées |
| | Pourcentage de requête SQL personnalisées exécutées sans erreurs | ≥ 80 % |
| | Nombre des décideurs qui accèdent aux tableaux de bord | ≥ au nombre de comptes créés pour les décideurs |
| **Évaluation** | Nombre de documents d'information (policy brief) produits | 1 par trimestre |

## 6.3 Indicateurs de suivi de mise en œuvre

Les indicateurs de suivi de mise en œuvre sont catégorisés pour une évaluation holistique de la plateforme, offrant une vision complète de ses performances et de son utilité :

**Tableau 5 : Indicateurs de suivi de mise en œuvre.**

| Catégorie | Indicateurs | Niveau de référence |
|---|---|---|
| **Formation** | Nombre de personnel IT formés | ≥ 2 par sectorielle membre de la plateforme |
| | Nombre d'intendants de données formés | ≥ 5 par sectorielle membre de la plateforme |
| | Nombre d'utilisateurs au niveau central formés | ≥ 5 par sectorielle membre de la plateforme |
| **Utilisation** | Nombre de réunions de revue des données tenues | 1 par trimestre |
| | Nombre de cas d'utilisation avancés configurés | ≥ au nombre de sectorielles impliquées |
| **Sécurisation** | Nombre des campagnes de sensibilisation menées | ≥ 1 par mois |
| | Nombre de personnel IT et intendants de données capacités en sécurisation des données | ≥ au nombre de comptes créés pour ces deux catégories d'utilisateurs |
| | Pourcentage des mesures de mitigation dans le cadre de la gestion des risques de mise en oeuvre | ≥ 90 % des risques identifiés |
| | Nombre d'audit de sécurité annuel | 1 fois par an |

## 6.4 Outils et méthodes de collecte

La collecte des données de suivi-évaluation s'opère à travers une approche digitalisée. Il s'agit d'une approche qui repose sur l'implémentation d'un système de collecte et

consolidation des données des différentes sources. Pour assurer le suivi de la mise en œuvre des activités, l'outil Kobo collect a été conçu et déployé, permettant une saisie structurée des données, lesquelles sont ensuite analysées et visualisées via un tableau de bord sur la plateforme COHIS. En ce qui concerne les indicateurs de performance, il y a un mélange des données automatique issues de la plateforme de monitoring des infrastructures serveurs, des sondages sur la satisfaction des utilisateurs (Kobo Collect) et des évaluations annuelles.

## 6.5 Fréquence et rapports

La production de rapports est rythmée selon une cadence définie pour garantir une réactivité optimale et une diffusion pertinente des informations issues des analyses approfondies en collaboration avec les partenaires techniques :

- **Rapports mensuels** des producteurs des données adressés au secrétariat permanent et à la Cellule Informatique ;
- **Rapports trimestriels** du Secrétariat permanent et de la Cellule Informatique adressés au Comité technique ;
- **Rapports semestriels** du comité technique adressés au comité d'orientation stratégique ;
- **Rapport annuel** du comité d'orientation stratégique aboutissant aux nouvelles orientations stratégiques.

## 6.6 Amélioration continue

Le mécanisme intègre une démarche proactive d'amélioration continue, essentielle à l'évolution et à la pérennité de la plateforme :

- Boucle de feedback : l'intégration systématique des retours utilisateurs permet de traiter efficacement les rapports de bogues et les demandes de nouvelles fonctionnalités ;
- Formations ciblées : la mise en place de sessions de renforcement des capacités est adaptée aux lacunes identifiées dans l'utilisation de la plateforme assurant une meilleure appropriation par les utilisateurs.

## 6.7 Plan de financement

Afin de soutenir le déploiement du système COHIS, sa maintenance, son développement technologique, ainsi que la bonne application de la gouvernance des données et la sécurisation de l'information, il est important de disposer d'un plan de financement adéquat. Ce financement devra couvrir les coûts opérationnels comprenant l'administration du système, la maintenance logicielle, le développement de nouvelles fonctionnalités, ainsi que des activités de terrain, notamment la formation du personnel et la mise en œuvre d'actions prioritaires pour l'opérationnalisation du système. La proposition de cadre budgétaire pluriannuel repris en annexe 17, permettrait de couvrir les ressources financières nécessaires au fonctionnement optimal du COHIS.

# GLOSSAIRE

## Anonymisation

L'anonymisation est un processus par lequel les données à caractère personnel sont transformées de manière irréversible afin qu'il ne soit plus possible d'identifier directement ou indirectement une personne, même en croisant les informations avec d'autres sources. Cette technique vise à protéger la vie privée des individus tout en permettant l'exploitation des données à des fins statistiques, scientifiques ou opérationnelles, sans que celles-ci ne soient soumises aux obligations légales liées aux données personnelles. Contrairement à la pseudonymisation, l'anonymisation élimine tout lien possible avec l'identité de la personne concernée, ce qui la rend particulièrement utile dans le cadre de la gouvernance des données pour réduire les risques juridiques et éthiques liés au traitement des informations sensibles.

## Chiffrement

Le chiffrement est un procédé de transformation des données lisibles (appelée texte en clair) en une forme codée (appelée texte chiffré) à l'aide d'un algorithme cryptographique et d'une clé. Cette opération vise à protéger la confidentialité des informations, en les rendant inintelligibles à toute personne non autorisée. Seules les entités disposant de la clé adéquate peuvent déchiffrer et accéder aux données originales. Le chiffrement peut être symétrique, lorsque la même clé est utilisée pour chiffrer et déchiffrer les données, ou asymétrique, lorsqu'un couple de clés distinctes (publique et privée) est utilisé. Le choix de la méthode dépend du niveau de sécurité requis, du contexte d'usage et des contraintes techniques.

## Data mesh

Le data mesh est une approche moderne de l'architecture des données qui met l'accent sur la décentralisation et la propriété des données orientée domaine. Il vise à relever les défis de la mise à l'échelle de la gestion et de la gouvernance des données dans les grandes organisations complexes en promouvant les principes suivants: 1) Propriété et architecture des données décentralisées orientées domaine : les données sont détenues par les équipes les plus proches d'elles, généralement celles qui les génèrent et les utilisent, plutôt que d'être gérées de manière centralisée ; 2) Les données en tant que produit : traiter les données avec le même niveau d'importance et de soin qu'un produit, en veillant à ce qu'elles soient de haute qualité, bien documentées et facilement accessibles ; 3) Infrastructure de données en self-service en tant que plateforme : fournir l'infrastructure et les outils nécessaires pour permettre aux équipes du domaine de gérer leurs données de manière autonome sans avoir à dépendre d'une équipe centrale ; 4) Gouvernance computationnelle fédérée : mettre en œuvre un modèle de gouvernance qui équilibre le besoin de normalisation et de conformité avec la flexibilité et l'autonomie des équipes décentralisées.

## Donnée

Une donnée est une information brute, factuelle et non interprétée, collectée à partir d'observations, mesures, enquêtes ou systèmes. Elle représente un élément de base qui, une fois analysé et mis en contexte, peut produire de l'information utile pour la prise de décision.

## Métadonnées

Les métadonnées, ou « données sur les données », comprennent des informations telles que la source des données, la date de leur dernière mise à jour, les personnes qui peuvent y accéder, etc. Une gestion efficace des métadonnées facilite la recherche, l'utilisation et la gestion des données dans l'entrepôt. Les définitions et la sémantique font également partie de ce qui constitue les métadonnées : elles apportent de la compréhension aux utilisateurs, un autre aspect clé de l'utilisabilité des données. Une bonne gestion des métadonnées peut inclure des outils tels qu'un catalogue de données pour donner un sens aux données utilisées quotidiennement en permettant la centralisation avec un dictionnaire de données, un traitement précis des données, un suivi de la traçabilité et un glossaire métier détaillé.

## Pare-feu

Un pare-feu est un dispositif de sécurité, matériel ou logiciel, qui contrôle les flux de données entrants et sortants d'un réseau informatique selon un ensemble de règles prédéfinies. Son rôle principal est de filtrer le trafic afin d'empêcher les connexions non autorisées et de protéger les systèmes informatiques contre les intrusions, les attaques externes ou les communications malveillantes. Dans un cadre de gouvernance des données, le pare-feu contribue à la protection de l'intégrité, de la disponibilité et de la confidentialité des données en agissant comme une barrière entre un réseau interne sécurisé et des réseaux externes potentiellement dangereux, comme Internet.

## Produit de données

Un produit de données au sens le plus simple est un ensemble d'indicateurs généralement présentés dans un tableau de bord conçu pour appuyer la prise de décision. De manière générale, il repose sur un jeu de données spécifique qui sert de base à des analyses, lesquelles sont ensuite transformées en informations claires, interprétables et directement utilisables par les décideurs.

## Self-Service

Une infrastructure de données en self-service est un système conçu pour permettre aux utilisateurs, souvent au sein d'une organisation, d'accéder, de gérer et d'utiliser indépendamment les données sans avoir besoin d'une assistance importante de la part des services informatiques. Il comprend généralement les fonctionnalités suivantes: 1) Accès et récupération des données : fournit des outils et des interfaces permettant aux utilisateurs de trouver et de récupérer facilement les données dont ils ont besoin ; 2) Traitement et analyse des données : offre aux utilisateurs la possibilité de nettoyer, transformer et analyser les données à l'aide d'outils conviviaux ; 3) Visualisation des données : permet aux utilisateurs de créer des graphiques, des tableaux de bord et d'autres représentations visuelles des données pour aider à la compréhension et à la prise de décision.

## Tableau de bord

Un tableau de bord est un outil visuel et interactif permettant de centraliser, synthétiser et visualiser en temps réel des informations essentielles, notamment des indicateurs clés de performance, afin de faciliter la prise de décision, le suivi opérationnel et le pilotage stratégique. Dans le contexte de la gouvernance des données, le tableau de bord joue un rôle fondamental en offrant une vue d'ensemble sur l'état et la qualité des données, la conformité

aux politiques internes, ainsi que sur les responsabilités et activités des différents acteurs impliqués dans la gestion des données.

# ANNEXES

## Tableau récapitulatif des annexes

## Annexe 1 : Contrôles technologiques du COHIS

### 1. Contexte

Afin de renforcer la sécurité et d'automatiser les processus, les contrôles technologiques sont essentiels pour protéger une plateforme d'intégration de données.

### 2. Liste des contrôles technologiques

Les contrôles technologiques comprennent les mesures suivantes :

- **Mesures de pseudonymisation et de chiffrement des données personnelles :**
  - Chiffrement des supports de données ;
  - Chiffrement des sites web (SSL) ;
  - Chiffrement des emails (TLS 1.2 ou 1.3) ;
  - Chiffrement des mots de passe et des clés.
- **Mesures pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience continue des systèmes de traitement et des services :**
  - Accord de non-divulgation avec les employés ;
  - Obligations de protection des données des employés ;
  - Accord de non-divulgation avec des tiers ;
  - Serveur de stockage / sauvegarde externe (Confirmé par le fournisseur d'hébergement) ;
  - Pare-feu ;
  - Logiciel anti-virus ;
  - Sauvegardes régulières des données ;
  - Surveillance des systèmes et des services ;
  - Systèmes RAID ;
  - Accord de maintenance ;
  - Tests réguliers des incidents informatiques ;
  - Stockage interne de copies/sauvegardes ;
  - Alimentation sans interruption (ASI), (À déterminer par le fournisseur d'hébergement selon l'offre) ;
  - Systèmes d'alarme incendie et fumée (À déterminer par le fournisseur d'hébergement selon l'offre) ;
  - Dispositifs de surveillance des températures (À déterminer par le fournisseur d'hébergement selon l'offre) ;
  - Alerte d'alarme en cas d'accès non autorisé (À déterminer par le fournisseur d'hébergement selon l'offre) ;
  - Équipement de lutte contre l'incendie (TDB par le fournisseur d'hébergement selon l'offre) ;
  - Alerte en cas d'accès non autorisé (TDB par le fournisseur d'hébergement selon l'offre) ;
  - Équilibrage de charge (TDB par le fournisseur d'hébergement selon l'offre) ;
  - Hébergement au niveau de CAMTEL.

- **Mesures pour garantir la capacité de restaurer la disponibilité et l'accès aux données personnelles en temps voulu en cas d'incident physique ou technique :**
  - Sauvegardes régulières de l'ensemble du système ;
  - Concept de sauvegarde des données ;
  - Tests de sauvegarde/récupération réguliers ;
  - Formation régulière du personnel informatique.
- **Processus pour tester et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement :**
  - Contrôles internes ;
  - Révision régulière des processus informatiques ;
  - Contrôles réguliers des employés.
- **Mesures pour l'identification et l'autorisation des utilisateurs :**
  - Authentification avec nom d'utilisateur / mot de passe ;
  - Séparation des rôles entre le système de test et le système de production ;
  - Gestion des permissions ;
  - Profils d'utilisateur ;
  - Politique de mot de passe ;
  - Limitation du nombre d'administrateurs ;
  - Séparation des rôles des utilisateurs ;
  - Gestion des droits par un administrateur ;
  - Différenciation entre les permissions.
- **Mesures pour la protection des données lors de la transmission :**
  - Utilisation de technologies de cryptage ;
  - Enrégistrement des activités et des événements ;
  - Cryptage des courriels (TLS 1.2 ou 1.3).
- **Mesures de protection des données lors du stockage :**
  - Cryptage des supports de donnée ;
  - Gestion des permissions ;
  - Limitation des accès ;
  - Enregistrement des actions et des événements ;
  - Limitation du nombre d'administrateurs ;
  - Stockage sécurisé des supports de données ;
  - Pare-feu.

- **Mesures pour garantir la sécurité physique des lieux où les données personnelles sont traitées :**
  - Hébergement au niveau de CAMTEL ;
  - Mesures pour assurer la traçabilité des événements ;
  - Utilisation de l'enregistrement automatique ;
  - Création de rapports d'incidents ;
  - Enregistrement au niveau des applications ;
  - Révision automatique des journaux ;
  - Révision manuelle régulière des journaux.
- **Mesures pour garantir la configuration du système, y compris la configuration par défaut :**
  - Politique de gestion de la configuration existante ;
  - Définition des configurations par défaut ;
  - Configuration par l'administrateur système ;
  - Enregistrement des modifications apportées aux configurations ;
  - Formation régulière du staff technique.
- **Mesures pour la gouvernance et la gestion interne des TI et de la sécurité informatique :**
  - Lignes directrices sur la sécurité informatique ;
  - Lignes directrices sur l'administration des TI ;
  - Audits / revues réguliers de conformité ;
  - Équipe informatique avec des rôles/responsabilités attribués.
- **Mesures pour la certification/l'assurance des processus et des produits :**
  - Aperçu des réglementations applicables aux produits/services/processus.
- **Mesures pour garantir la minimisation des données :**
  - Définition claire de l'objectif du traitement ;
  - Limitation de la collecte aux données strictement nécessaires.
- **Mesures pour garantir la qualité des données :**
  - Profilage et classification des données ;
  - Contrôle des données entrantes ou nouvelles ;
  - Enregistrement de l'entrée/changement des données ;
  - Attribution des droits pour la saisie des données ;

- Traçabilité des utilisateurs lors de la saisie ou du changement des données ;
- Réduction des redondances dans les données ;
- Identification des besoins en données ;
- Application des mesures pour garantir la qualité des données.

- **Mesures pour assurer la rétention limitée des données :**
  - Formation régulière ;
  - Révision et évaluation régulières des données stockées.
- **Mesures pour garantir la responsabilité :**
  - Formation / Sensibilisation ;
  - Vérifications et audits réguliers ;
  - Équipe responsable de la protection des données ;
  - Orientations et soutien aux employés ;
  - Politiques de confidentialité appropriées ;
  - Rapports d'audit et mesures documentés ;
  - Implication du responsable de la sécurité des données.
- **Mesures pour permettre la portabilité des données et garantir l'effacement :**
  - Stockage dans un format structuré ;
  - Facilitation de la portabilité des données.

## Annexe 2 : Normes de qualité des données, y compris les normes et cadres des métadonnées

La qualité des données et la gestion des métadonnées sont cruciales pour garantir à la fois la fiabilité et l'interopérabilité sémantique des données entre les sources de données. Par conséquent, des processus robustes de gestion de la qualité des données et des métadonnées doivent être appliqués comme l'un des piliers cruciaux de la gouvernance du COHIS. Le cadre de gestion de la qualité des données et de l'interopérabilité sémantique appliqué dans le cadre de gouvernance des données du COHIS, est construit sur les normes internationales ISO 8000 et ISO/IEC 11179.

Ainsi, le cadre repose sur deux piliers :

1. **Assurance qualité des données ;**
2. **Gestion et conformité des métadonnées.**

### 1. Assurance qualité des données

La norme ISO 8000 définit la qualité des données selon les dimensions suivantes :

- **Exactitude :** cette dimension fait référence à la mesure dans laquelle les données décrivent correctement l'objet ou l'événement du monde réel qu'elles représentent. Par exemple, si le résultat d'un test de laboratoire indique la présence d'un gène spécifique de la résistance aux antimicrobiens dans un isolat bactérien, les données sont exactes si elles reflètent véritablement le résultat du test sans erreur d'étiquetage ou d'interprétation. **Exemple** : une coordonnée de géolocalisation saisie pour une épidémie doit pointer vers la zone touchée réellement.
- **Complétude :** l'exhaustivité évalue si toutes les données requises sont présentes. Dans un dossier de surveillance, cela signifie que tous les champs obligatoires, tels que l'espèce, le diagnostic, la date de détection, sont remplis et qu'aucun n'est manquant. **Exemple** : une étude de cas dont le nom de l'espèce ou le résultat de l'essai ne contient pas le nom de l'espèce serait considérée comme incomplet.
- **Consistance :** les données sont cohérentes lorsqu'elles sont logiquement cohérentes et qu'elles ne se contredisent pas entre les ensembles de données, le temps ou les systèmes. Il s'agit de contrôles internes (par exemple, une date de naissance ne peut pas être postérieure à une date de diagnostic) et de contrôles externes (par exemple, le même identifiant doit toujours faire référence à la même entité). **Exemple** : un code de région doit toujours être mappé au même nom géographique dans chaque enregistrement.
- **Ponctualité :** cette dimension mesure si les données sont disponibles et à jour en cas de besoin. Dans des domaines en évolution rapide comme la santé publique, les données perdent de la valeur si elles sont retardées. **Exemple** : les retards dans la déclaration des cas de rage au système central réduisent l'utilité des données pour une réponse immédiate.
- **Validité :** elle évalue si les données sont conformes à des formats, des normes ou des règles métier définis. Il vérifie si les valeurs se trouvent dans des domaines acceptables ou répondent aux exigences syntaxiques. **Exemple** : un champ pour les résultats d'un test de résistance aux antimicrobiens ne doit accepter que les valeurs d'une liste prédéfinie (par exemple, « Résistant », « Sensible », « Intermédiaire »).

- **Unicité :** il s'agit de l'absence de doublons dans les enregistrements. Les doublons peuvent fausser les statistiques et induire les décideurs en erreur. **Exemple** : si le même animal est signalé deux fois sous des identifiants différents, les données manquent d'unicité.
- **Provenance (lignée) :** la provenance fait référence à l'historique documenté d'un élément de données, y compris son origine, ses transformations et sa propriété. La norme ISO 8000 souligne l'importance de pouvoir retracer l'origine des données et la manière dont elles ont été modifiées. **Exemple** : le fait de savoir que les résultats des tests de laboratoire ont été produits dans une installation certifiée à une date précise renforce la confiance dans leur fiabilité.
- **Cohérence de la représentation :** cette dimension garantit que les données sont présentées de manière uniforme, en particulier lorsque le même concept est réutilisé dans des systèmes ou des ensembles de données. **Exemple** : les réponses « Oui/Non » ne doivent pas apparaître dans des formats mixtes tels que « O/N », « 1/0 » ou « Vrai/Faux » dans le même champ.
- **Accessibilité :** l'accessibilité concerne la facilité avec laquelle les utilisateurs peuvent récupérer et utiliser les données. Les données doivent être disponibles par le biais d'interfaces appropriées et suffisamment documentées pour être réutilisées. **Exemple** : Les agents de santé publique devraient être en mesure de récupérer et d'interpréter les données sur les dangers environnementaux via l'interface de la plateforme sans avoir besoin d'un soutien technique.
- **Pertinence :** La pertinence décrit si les données sont appropriées et utiles pour la tâche prévue. Cela dépend du contexte d'utilisation et des besoins des parties prenantes. **Exemple** : L'inclusion de registres détaillés sur l'utilisation des antimicrobiens est très pertinente dans l'analyse de la RAM, mais peut ne pas l'être pour les rapports sur les tendances des éclosions de zoonoses.

## 2. Gestion de la qualité des données – rôles et responsabilités

Les utilisateurs sont responsables de la qualité des données de leurs produits de données respectifs. Les intendants des données aideront les utilisateurs à effectuer des contrôles de la qualité des données.

Ainsi, les contrôles de qualité des données suivants sont obligatoires pour tous les produits de données et doivent être configurés en tant qu'analyse automatique de la qualité des données dans le module de visualisation du COHIS : complétude, consistance, validité, cohérence de la représentation.

## 3. Gestion et conformité des métadonnées

Les intendants des données tiendront à jour un registre et un dictionnaire de métadonnées. Le registre de métadonnées stocke, gère et partage les *métadonnées,* c'est-à-dire les données sur les données. Il fonctionne comme un catalogue central où les définitions, les formats, les relations et les contraintes des éléments de données sont clairement documentés et normalisés.

Le registre de métadonnées contient des entrées pour des éléments de données individuels (tels que « Âge du patient », « Espèce animale » ou « Résultat du test ») et décrit leur :

- Signification (définition conceptuelle) ;
- Format (type de données, longueur, etc.) ;
- Valeurs autorisées (par exemple, listes codées, énumérations, classifications) ;
- Relations (p. ex., comment un élément de données est lié à un autre) ;
- Propriété (qui est responsable de la définition et de la maintenance).

Le registre ne stocke pas les valeurs de données réelles (par exemple, les noms des patients ou les résultats de laboratoire), mais plutôt les définitions et les règles qui régissent la façon dont ces valeurs sont capturées, représentées et interprétées.

Les intendants de données sont chargés d'enregistrer les nouveaux éléments de données dans le registre des métadonnées et de réviser les formats au fil du temps si nécessaire.

Les producteurs de données sont tenus de respecter les normes de métadonnées décrites dans le registre lors de la création d'un nouveau produit de données, et les intendants des données doivent valider la conformité des nouveaux produits de données avec les normes de métadonnées décrites dans le registre.

Les utilisateurs peuvent consulter le registre des métadonnées pour mieux comprendre les éléments de données dans les différents ensembles de données qu'ils consomment.

En plus de la tenue à jour et de la conformité au registre des métadonnées, chaque produit de données doit contenir une note de description du produit de données. Il s'agit d'un récit ou d'une documentation structurée qui fournit des informations clés sur le produit de données, expliquant ce qu'il contient, comment il a été créé/comment les données ont été collectées et comment elles doivent être interprétées. Il aide les utilisateurs à comprendre le contexte, les limites et la pertinence des données.

La note descriptive doit contenir les éléments suivants :

- Titre et identificateur : nom clair et unique de l'ensemble de données, éventuellement accompagné d'un identificateur unique ou d'une URI (*Uniform Resource Identifier*) ;
- Résumé : un court récit expliquant l'objectif et la portée de l'ensemble de données ;
- Origine et propriété : qui a créé ou collecté les données, y compris l'institution responsable et ses coordonnées ;
- Couverture temporelle et spatiale : quand et où les données ont été collectées (par exemple, 2022-2023, région de l'Extrême-Nord du Cameroun) ;
- Structure et format des données : description de la structure (p. ex., tabulaire, géospatiale, JSON), des formats de fichiers (CSV, XML, etc.) et du schéma, le cas échéant ;
- Variables et définitions : une brève explication de chaque variable ou champ clé, y compris les unités de mesure, les systèmes de codage et les types de données ;

- Méthodologie de collecte de données : explication de la façon dont les données ont été recueillies, p. ex., au moyen d'enquêtes, d'analyses de laboratoire, de relevés de capteurs ou de dossiers administratifs ;
- Qualité et limites : notes sur l'exactitude et l'exhaustivité des données, les biais connus et les mises en garde concernant l'interprétation.

### 4. Liste de contrôle pour les intendants des données

Pour garantir la qualité des données et la conformité aux normes de métadonnées, les intendants des données doivent mettre en œuvre les tâches suivantes lors de la validation des nouveaux produits de données :

- Analyse de la qualité des données, traitement des données et configuration des visualisations/tableaux de bord ;
- Validation des métadonnées du nouveau produit de données par comparaison avec les éléments de données du registre des métadonnées ;
- Validation de la note de description du produit de données.

## Annexe 3 : Accord de confidentialité et d'utilisation de la plateforme COHIS.

### 1. Présentation

Bienvenue sur le *Cameroon One Health Information System* (COHIS), la plateforme nationale d'intégration, de partage et d'analyse des données issues des secteurs de la santé humaine, animale, végétale et environnementale. Le présent contrat d'utilisation décrit les responsabilités et les obligations de tous les utilisateurs autorisés à accéder à COHIS.

En accédant ou en utilisant COHIS, vous reconnaissez avoir lu, compris et accepté de vous conformer aux termes du présent accord, qui est guidé par les lois camerounaises et les normes internationales, notamment :

#### 1.1. Normes et stratégies internationales

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;

- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;
- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité.

### 1.2. Lois et actes du Cameroun

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

## 2. Définitions

- **Utilisateur :** toute personne autorisée à accéder à COHIS ;
- **Données :** toute donnée de santé humaine, animale, végétale ou environnementale stockée, traitée ou transmise via COHIS ;
- **Données sensibles :** toutes les données dont la divulgation, la modification ou la perte non autorisée pourraient nuire à la santé publique, aux individus ou aux institutions.

## 3. Obligations de l'utilisateur

### 3.1. Protection des données

- Les utilisateurs doivent s'assurer que les informations personnellement identifiables sont traitées conformément aux lois camerounaises sur la protection des données. Ainsi, les utilisateurs sont priés de s'abstenir de partager des données personnelles et sensibles dans la mesure du possible sur COHIS. Dans le cas où les utilisateurs souhaitent partager des données personnellement identifiables sur la plateforme, ils doivent demander le partage de ces données auprès d'un intendant de données COHIS qui sera chargé de valider ou de refuser le partage de ces données et veillera à ce que les dispositions nécessaires à la protection des données soient mises en place ;
- Les utilisateurs doivent appliquer des méthodes d'anonymisation ou de pseudonymisation des données dans la mesure du possible ;
- Les utilisateurs doivent éviter toute divulgation ou accès non autorisé à toute donnée obtenue par l'intermédiaire de COHIS.

### 3.2. Gestion de la qualité des données

- Les utilisateurs doivent saisir et conserver des données exactes, complètes, cohérentes et opportunes ;
- Il incombe à l'utilisateur de valider les données avant de les soumettre et de corriger rapidement les erreurs identifiées ;
- Les utilisateurs doivent consulter le registre des métadonnées COHIS pour s'assurer que les données et les métadonnées respectent les normes de qualité reconnues.

### 3.3. Sécurité de l'information

- Les utilisateurs doivent utiliser des méthodes d'authentification sécurisées et préserver la confidentialité des identifiants de connexion. Par conséquent, les utilisateurs sont priés de ne pas enregistrer leurs identifiants de connexion sur des applications et des appareils mal protégés ou non protégés ;
- Les utilisateurs ne sont pas autorisés à partager leurs identifiants d'accès avec qui que ce soit ;
- Les utilisateurs doivent immédiatement signaler toute violation présumée de la sécurité des données, tout accès non autorisé ou toute perte de données à l'administrateur de la plateforme COHIS.

## 4. Règles d'accès et d'utilisation

- L'accès au SISCO est fondé sur les rôles et accordé en fonction des mandats de l'établissement ;
- Les utilisateurs ne doivent pas utiliser la plateforme à des fins non autorisées, y compris la manipulation de données, l'extraction pour des recherches non autorisées ou le partage avec des tiers sans autorisation ;
- Les journaux d'accès peuvent être vérifiés pour garantir la conformité avec le présent accord.

## 5. Confidentialité

- Tous les utilisateurs doivent traiter les informations consultées par l'intermédiaire de COHIS comme confidentielles, à moins qu'elles ne soient explicitement marquées comme publiques ;
- Les utilisateurs ne doivent pas partager de données confidentielles en dehors des flux de travail institutionnels autorisés sans autorisation écrite préalable ;
- L'obligation de confidentialité survit à la résiliation de l'accès au système.

## 6. Application de la loi et sanctions

La violation de cet accord peut entraîner :

- Suspension ou révocation définitive de l'accès à COHIS ;
- Mesures disciplinaires prises par l'employeur ou l'établissement de l'usager ;
- Action en justice conformément à la loi camerounaise.

## 7. Reconnaissance et consentement

En vous inscrivant ci-dessous ou en utilisant la plateforme COHIS, vous confirmez que vous :

- Avoir lu et compris les termes du présent accord ;
- Accepter de se conformer à toutes les obligations et restrictions décrites dans les présentes ;
- Comprendre les conséquences de la non-conformité.

**Nom :**_____

**Organisation :**_____

**Rôle/Titre :**_____

**Date :**_____

**Signature :** _____

## Annexe 4 : Termes de référence de l'intendant de données.

### 1. Contexte

Le Système d'Information *One Health* (COHIS) est une plateforme nationale d'intégration de données conçue pour soutenir la collaboration multisectorielle entre les secteurs de la santé humaine, animale, végétale et environnementale. La plateforme permet le partage de données, l'interopérabilité et la prise de décision fondée sur des données probantes, alignées sur les lois camerounaises et les normes internationales, telles que :

#### 1.1. Normes et stratégies internationales

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;
- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;

- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité.

### 1.2. Lois et actes du Cameroun

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

Pour maintenir des données de haute qualité, fiables et sécurisées au sein du système, COHIS s'appuie sur le rôle essentiel des intendants de données.

## 2. Objet du rôle

L'intendant des données a pour but de veiller à l'application du Cadre de Gouvernance des Données et Sécurité d'information du COHIS. Ainsi, les intendants de données garantissent l'exactitude, la cohérence, l'exhaustivité et la sécurité des données au sein du COHIS. Ils sont chargés de superviser la mise en œuvre des principes de qualité des données, de normes des métadonnées et de pratiques de sécurité de l'information au niveau opérationnel. Il rend compte directement au responsable de la gouvernance des données et agit en tant que première ligne de contrôle pour assurer l'intégrité et la conformité des données saisies et conservées dans le système.

## 3. Principales responsabilités

Les intendants de données sont des experts techniques qui gèrent l'ensemble des informations détenues dans le système. Ils travaillent avec les propriétaires de données afin de garantir des données fiables, sécurisées et conformes aux normes de la qualité des données.

### 3.1. Validation et maintenance de produits des données

Les intendants de données sont responsables de la validation des nouveaux produits de données. Le responsable de la gouvernance des données veille à ce que tous les nouveaux produits de données aient été validés par un intendant de données.

L'intendant de données veille :

- Au respect des lois et règles en matière de protection des données, en particulier si les données comprennent des informations personnellement identifiables ;
- Au respect des normes de qualité des données et métadonnées (annexes 2 et 7) ;
- A la configuration avec le producteur de données des indicateurs automatiques de contrôle de la qualité des données pour le produit de données ;
- A la cohérence de la description des produits de données, afin de permettre une traçabilité des données appropriée et l'exhaustivité des données pour les autres utilisateurs. Il s'assure de la validation de la fiche de description des données (annexe 6) ;
- A l'établissement des règles d'accès à un produit de données : le producteur de données définit les droits d'accès en concertation avec l'intendant de données. Ce dernier communiquera les droits d'accès au responsable de la gouvernance des données et s'assurera de sa mise en place.

### 3.2. Conformité à la sécurité de l'information

L'intendant de données :

- Signale toute violation de données, tout modèle d'accès suspect ou toute violation des protocoles de traitement des données ;
- S'assure du traitement confidentiel et sécurisé des données de santé personnellement identifiables ou sensibles, conformément aux lois sur la protection des données.

### 3.3. Collaboration et rapports

L'intendant de données :

- Travaille en étroite collaboration avec les équipes techniques, les experts du domaine et les fournisseurs de données pour améliorer la gestion du cycle de vie des données ;
- Fournit des mises à jour régulières et des rapports d'incidents au responsable de la gouvernance des données ;
- Forme et accompagne les producteurs de données sur la qualité des données et les normes de métadonnées.

## 4. Supervision et responsabilisation

L’intendant de données :

- Relève de l’unité de traitement ou l’unité de sécurité ;
- Veille au respect des normes strictes de confidentialité et d'éthique dans le traitement des données.

## Annexe 5 : Termes de référence du responsable de gouvernance des données.

### 1. Contexte

Le *Cameroon One Health Information System* (COHIS) est une plateforme nationale d'intégration de données conçue pour soutenir la collaboration multisectorielle entre les secteurs de la santé humaine, animale et environnementale. La plateforme permet le partage de données, l'interopérabilité et la prise de décision fondée sur des données probantes, alignées sur les lois camerounaises et les normes internationales, telles que :

#### 1.1. Normes et stratégies internationales

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;
- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;

- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité.

### 1.2. Lois et actes du Cameroun

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

## 2. Objet du rôle

Le responsable de la gouvernance des données du COHIS est en charge de la gestion de la politique globale de la plateforme. Il est le garant stratégique de la qualité, de la sécurité et de la valeur des données utilisées au sein de la plateforme. Il assure un leadership transversal pour instaurer une culture de gouvernance responsable et coordonnée des données, alignée sur les objectifs nationaux de santé publique, de sécurité sanitaire et de développement durable :

- Développement et pilotage de la stratégie de gouvernance des données : le responsable conçoit, développe et met en œuvre la stratégie de gouvernance des données du COHIS. Il veille à ce que cette stratégie soit en parfaite cohérence avec les priorités et objectifs organisationnels plus larges du *One Health*, notamment en matière de surveillance, d'alerte précoce, de recherche, de transparence et de redevabilité ;
- Nomination des unités de traitement et de sécurisation des données : en tant qu'autorité fonctionnelle, le responsable de la gouvernance nomme les unités de traitement et de sécurisation des données. Il veille sur leur mandat, leur périmètre d'action, leurs

obligations de résultats, et supervise leur coordination pour garantir l'harmonisation des pratiques à l'échelle de la plateforme ;

- Encadrement des rôles et responsabilités liés à la donnée : il veille sur le respect des obligations des différents acteurs de la gouvernance des données (intendants de données et point focal COHIS) et veille à la mise en place des mécanismes de redevabilité, coordination et communication entre eux ;
- Soutien à la culture organisationnelle autour des données : il joue un rôle de mobilisateur, sensibilisant les décideurs, techniciens et partenaires à l'importance de la gouvernance des données. Il promeut une culture fondée sur la valeur stratégique de la donnée et sur la prise de décision fondée sur des preuves fiables et partagées ;
- Suivi stratégique et reporting: le responsable assure un suivi régulier de l'implémentation du cadre de gouvernance des données et sécurité des informations du COHIS et propose des ajustements en fonction de l'évolution du contexte.

## Annexe 6 : Modèle de description des données.

### 1. Informations générales sur le jeu de données

| Titre du jeu de données | [nom clair et unique de l'ensemble de données, éventuellement accompagné d'un identificateur unique ou d'une URI] |
|---|---|
| **Date de création (jj-mm-aaaa)** | [Insérer la date] |
| **Créé par (Institution/Auteur)** | [Insérer le nom de l'établissement ou du créateur des données] |
| **Niveau de sensibilité des données** | ☐ Public ☐ Restreint ☐ Confidentiel ☐ Personnel/Identifiable |

### 2. Résumé

[Un court récit expliquant l'objectif et la portée de l'ensemble de données.]

| Couverture temporelle et spatiale | [Quand et où les données ont été collectées (par exemple, 2022-2023, région de l'Extrême-Nord du Cameroun).] |
|---|---|
| **Structure et format des données** | [Description de la structure (p. ex., tabulaire, géospatiale, JSON), des formats de fichiers (CSV, XML, etc.) et du schéma, le cas échéant] |
| **Méthodologie de collecte de données** | [Explication de la façon dont les données ont été recueillies, p. ex., au moyen d'enquêtes, d'analyses de laboratoire, de relevés de capteurs ou de dossiers administratifs.] |
| **Qualité et limites** | Notes sur l'exactitude et l'exhaustivité des données, les biais connus et les mises en garde concernant l'interprétation. |

### 3. Institutions autorisées et rôles des utilisateurs

| Nom de l'établissement | Secteur (Humain/ Animal/ Environnement) | Rôle d'utilisateur (spectateur, éditeur, administrateur) | Description des droits d'accès |
|---|---|---|---|
| **[p. ex., Ministère de la Santé]** | Humain | Éditeur | Afficher les tendances épidémiologiques agrégées |
| **[p. ex., Ministère de l'Élevage]** | Animal | Éditeur | Saisir et mettre à jour les données au niveau des cas sur les zoonoses |
| **[p. ex., Institut de recherche X]** | Environnemental | Spectateur | Accès pour la modélisation des risques écologiques |
| **[p. ex., bureau de pays de l'OMS]** | Humain | Spectateur | Accès à l'exportation de rapports de données hebdomadaires intégrés |

## 4. Variables et définitions

| **Nom de la variable (colonne)** | **Présence dans le registre de métadonnées (Oui, Non),** *si présent dans le registre, se passer de la description* | **Description de la donnée (définir la donnée, a quoi elle renvoie, etc…..)** |
|---|---|---|
| **[p. ex., région]** | | |
| **[p. ex., nombre de cas]** | | |

## Annexe 7 : Registre des métadonnées

### 1. Objectif

Le registre de métadonnées est un référentiel structuré qui vise à standardiser la définition, la description, la gestion et l'utilisation des données à travers les systèmes d'information. Selon le standard ISO/IEC 11179, son objectif principal est de faciliter l'interopérabilité sémantique entre les systèmes, en assurant que tous les acteurs comprennent les données de la même manière, même lorsqu'elles sont échangées ou utilisées dans des contextes différents.

Il permet notamment de :

- Fournir une description univoque des éléments de données ;
- Harmoniser la terminologie à travers les secteurs ;
- Soutenir la gouvernance des données et la qualité des données ;
- Favoriser la réutilisation de définitions existantes ;
- Servir de base à la validation des jeux de données produits.

Dans le cadre du COHIS, le registre de métadonnées selon ISO/IEC 11179 joue un rôle central pour garantir que :

- Les différentes administrations de santé (humaine, animale, végétale et environnementale) utilisent des définitions de données cohérentes pour la surveillance intégrée des maladies ;
- Les données des systèmes hétérogènes (DHIS2, CAHIS, etc.) puissent être consolidées de manière compréhensible et exploitable ;
- Les indicateurs, les éléments de données, les classifications des pathogènes et les localisations soient clairement définis, versionnés et gouvernés.

### 2. Modèle de registre des métadonnées

| Identifiant | Nom de l'élément | Définition | Domaine de valeurs | Type de donnée | Source | Statut | Version |
|---|---|---|---|---|---|---|---|
| **MD001** | sexe_patient | Sexe du patient au moment de l'enregistrement | [M, F, Autre] | Texte court | MoH / DHIS2 | Approuvé | v1.2 |
| **MD002** | espèce_animale | Espèce de l'animal suspecté ou confirmé | Code OIE (Ovis aries, Bos taurus, etc.) | Code | MINEPIA | En cours | v0.9 |
| **MD003** | date_onset | Date de début des symptômes | jj-mm-aaaa | Date | SORMAS | Approuvé | v1.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **MD004** | code_localité | Code standardisé des localités selon INS | ISO 3166-2:CM | Code | INS | Approuvé | v2.1 |

## 3. Maintenance et application du registre des métadonnées

Les intendants de données sont des responsables désignés chargés de :

- **Gérer les métadonnées :**
  - Proposer, documenter et valider les nouveaux éléments de données ;
  - Définir les règles de codage, les unités de mesure, les contraintes, etc.
  - Veiller à la qualité sémantique des métadonnées.
- **Mettre à jour le registre :**
  - Documenter chaque changement (ex. nouvelle version, retrait, fusion) ;
  - Suivre un processus de gouvernance (soumission → validation → publication) ;
  - Assurer la traçabilité (qui a modifié quoi, quand, pourquoi).
- **Assurer la conformité :**
  - Vérifier que les jeux de données produits (rapports, tableaux de bord, exports) utilisent les définitions validées ;
  - Utiliser des mécanismes d'audit ou de validation automatique (par exemple, scripts de contrôle qualité).

## Annexe 8 : Cadre de risque.

### 1. Objectif

Le registre de métadonnées est un référentiel structuré qui vise à standardiser la définition, la description, la gestion et l'utilisation des données à travers les systèmes d'information. Selon le standard ISO/IEC 11179, son objectif principal est de faciliter l'interopérabilité sémantique entre les systèmes, en assurant que tous les acteurs comprennent les données de la même manière, même lorsqu'elles sont échangées ou utilisées dans des contextes différents.

Il permet notamment de :

- Fournir une description univoque des éléments de données ;
- Harmoniser la terminologie à travers les secteurs ;
- Soutenir la gouvernance des données et la qualité des données ;
- Favoriser la réutilisation de définitions existantes ;
- Servir de base à la validation des jeux de données produits.

### 2. Application et mise à jour du cadre de gestion des risques

Ce cadre est appliqué comme un cycle continu intégré au développement, au déploiement et aux opérations de la plateforme. Il commence par l'identification des risques lors de la conception du système et se poursuit par des évaluations régulières des risques, la collecte de renseignements sur les menaces, les tests de sécurité et la surveillance des performances.

Le processus de gestion des risques est appliqué conformément à la méthodologie de l'ISO/IEC 27005, garantissant une approche systématique et reproductible de l'identification, de l'évaluation, du traitement et de la surveillance des risques.

Les mises à jour sont effectuées :

- Annuellement, dans le cadre d'audits et d'examens de sécurité programmés ;
- Après des changements majeurs de plateforme, tels que de nouveaux modules ou API ;
- À la suite d'incidents, en vue d'intégrer les leçons apprises ;
- En conformité avec l'évolution des exigences légales et réglementaires.

Le cadre est géré en collaboration par le responsable de la sécurité de l'information (RSI), les points focaux et les équipes informatiques des ministères ; sous la supervision du responsable de la gouvernance des données.

### 3. Catégories de risques, menaces et mesures d'atténuation

La méthodologie utilisée pour classer la probabilité des événements et la gravité de l'impact suit une approche structurée consistant à : identifier les risques, définir les critères de

probabilité, définir les critères d'impact, ressortir le niveau de risque, établir la matrice des risques et identifier les mesures d'atténuation.

- La probabilité d'occurrence (à quelle fréquence il peut survenir) ;
- L'impact potentiel (gravité des conséquences sur les opérations ou la confidentialité) ;
- Le niveau de risque global (calculé en croisant impact et probabilité) ;
- Les mesures de sécurité appropriées à mettre en place pour atténuer ou maîtriser ce risque.

Les critères de vraisemblance sont les suivants :

- **Faible :** ne s'est pas produit au cours des 5 dernières années dans des projets similaires au Cameroun et ne se produit que dans des circonstances inhabituelles ;
- **Moyen :** s'est produite occasionnellement mais rarement lors d'interventions similaires au Cameroun ;
- **Élevé :** a eu lieu dans des projets similaires au Cameroun ;
- **Sévère :** se produit régulièrement et est attendue au Cameroun.

Les critères d'impact sont les suivants :

- **Faible :** petit retard ou dépassement de coût; Facilement gérable ;
- **Moyen :** perturbation notable nécessitant une coordination avec plusieurs acteurs ;
- **Élevé :** incidence sur plusieurs activités/volets du COHIS ;
- **Sévère :** la réussite du COHIS est menacée.

Pour évaluer la probabilité d'événements potentiels, l'évaluation est basée sur des données historiques du projet et sur le jugement d'experts des parties prenantes impliquées dans la gestion de la sécurité de l'information. Pour évaluer la gravité de l'impact des événements potentiels, l'évaluation est fondée sur l'identification des résultats touchés et sur l'estimation des coûts et des retards attribuables à ces impacts.

Le niveau de risque est le résultat de la combinaison de probabilité - impact. Les critères de niveau de risque sont les suivants :

- **Faible × Faible = Faible :** Risque mineur avec peu d'incidence sur le système ou les opérations, et peu probable ;
- **Faible × Moyen = Modeste :** Risque modeste avec incidence modérée sur le système ou les opérations ;
- **Élevé × Faible ; Moyen × Moyen ; Faible × Élevé = Moyenne :** Risque avec un impact Moyen ou une probabilité faible à moyenne ;
- **Élevé × Moyenne = Modéré :** Risque avec un impact significatif (altération, violation de confidentialité, indisponibilité prolongée) et une probabilité Moyenne à élevée ;
- **Élevé × Élevé = Élevé :** Risque avec un impact élevé ;

- **Élevé x Sévère = Majeur :** Risque avec un impact majeur ;
- **Sévère x Sévère = Critique :** Risque dont l'impact est très élevé (perte de données sensibles, paralysie complète) et la probabilité d'occurrence est élevée.

## Catégories de risques, menaces et mesures d'atténuation :

| Catégorie de risque | Risques et menaces potentiels | Probabilité | Gravité | Niveau de risque | Mesures d'atténuation |
|---|---|---|---|---|---|
| **Gouvernance et politiques** | Absence de gouvernance formelle des données | Moyenne | Élevé | Modéré | Validation de cadre de gouvernance des données et sécurité des informations |
| | Ambiguïté dans la prise des décisions pour réagir aux incidences des attaques ou non-respect des lois | Moyenne | Élevé | Modéré | |
| | Ambiguïté dans la propriété des données | Moyenne | Moyenne | Moyenne | Assurer que la note de description et autorisation de partage des données soit faites pour chaque jeu de données |
| **Contrôle d'accès** | Accès non autorisé | Moyenne | Élevé | Modéré | Appliquer le contrôle d'accès basé sur les rôles (RBAC) |
| | Élévation de privilèges | Faible | Élevé | Moyenne | Mettre en oeuvre « principe du moindre privilège » |
| | Comptes dormants non désactivés | Moyenne | Moyenne | Moyenne | Automatiser la désactivation des utilisateurs après une inactivité<br>Auditer les comptes des utilisateurs d'une manière régulière |
| **Réseau et infrastructure** | Communication non cryptée | Moyenne | Moyenne | Moyenne | Appliquer l'utilisation de TLS |
| | Attaques DDoS ou DNS | Faible | Moyenne | Modeste | Utiliser des services d'atténuation CDN/DDoS et des |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | applications de monitoring (SIEM) |
| | Pare-feu ou routeurs mal configurés | Faible | Moyenne | Modeste | Audits réguliers de la configuration du réseau |
| **Sécurité des terminaux et des utilisateurs** | Logiciels malveillants/ransomwares | Elevé | Moyenne | Modéré | Installez des outils de protection des terminaux<br>Appliquer MFA pour les comptes administrateurs |
| | Appareils perdus ou volés | Élevé | Faible | Moyenne | Ne sauvegarde pas des données sensibles sans chiffrement sur les appareils<br>Appliquer MFA pour les comptes administrateurs |
| | Attaques de phishing ou d'ingénierie sociale | Elevé | Moyenne | Modéré | Formez les utilisateurs au phishing et à l'informatique sécurisée<br>Appliquer MFA pour les comptes administrateurs |
| **Sécurité des applications** | Attaques par injection (par exemple, SQL, XSS) | Moyenne | Élevé | Modéré | Suivre les principes de codage sécurisé de l'OWASP |
| | Authentification brisée | Moyenne | Élevé | Modéré | Exiger les mots de passe complexes<br>Limiter les tentatives de connexion<br>Appliquer MFA pour les comptes administrateurs |
| | Exposition de l'API sans limitation de débit | Moyenne | Élevé | Modéré | Sécuriser toutes les API avec des jetons et une limitation |
| **Sécurité et confidentiali** | Accès ou modification non autorisés des données | Moyenne | Moyenne | Moyenne | Chiffrer les données sensibles |

| | | | | | |
|---|---|---|---|---|---|
| **té des données** | | | | | Mettre en œuvre le modèle de définition des accès aux données |
| | Manque d'auditabilité | Moyenne | Moyenne | Moyenne | Activer les journaux d'audit détaillés |
| **Risque lié aux tiers** | Dépendances logicielles non sécurisées | Moyenne | Moyenne | Moyenne | Utiliser des projets open-source approuvés (Fondation Apache) |
| | Absence de SLA avec les fournisseurs d'hébergement | Moyenne | Élevé | Modéré | Définir des SLA pour les fournisseurs |
| | Portes dérobées dans les composants open source | Moyenne | Élevé | Modéré | Effectuer des revues SBOM (Software Bill of Materials) |
| **Reprise après sinistre et continuité** | Panne matérielle<br>Une cyberattaque efface les données | Moyenne | Élevé | Modéré | Mettre en œuvre des sauvegardes automatisées hors site<br>Tester la récupération des sauvegardes régulièrement |
| **Conformité et risque juridique** | Désalignement avec la loi camerounaise ou les politiques de l'UA en matière de données | Moyenne | Élevé | Modéré | Nommer un « responsable de la gouvernance des données »<br>Effectuer des audits de conformité annuels |
| | Exportation de données sans autorisation | Moyenne | Moyenne | Moyenne | Mettre en place le processus standardisé de mise à disposition des données |
| **Surveillance et réponse** | Détection tardive de l'atteinte | Moyenne | Élevé | Modéré | Utiliser le SIEM (par exemple, Wazuh) |
| | Manque de responsabilité pour la réponse aux incidents | Moyenne | Élevé | Modéré | Tenir à jour la documentation |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | d'intervention en cas d'incident |
| **Risque lié aux ressources humaines** | Manque de personnel de sécurité formé | Moyenne | Moyenne | Moyenne | Former sur la cybersécurité |
| | Un taux de rotation élevé entraîne une perte de connaissances | Moyenne | Moyenne | Moyenne | |
| **Risque lié à la gestion du changement** | Mises à jour mal testées | Faible | Moyenne | Modeste | Appliquer les pratiques DevSecOps |
| | Déploiements de fonctionnalités incontrôlés | Faible | Moyenne | Modeste | Utiliser des pipelines CI/CD avec des tests automatisés |
| | Absence de mécanismes de retour en arrière | Faible | Moyenne | Modeste | Maintenir des environnements contrôlés par version |
| **Risque de sécurité physique** | Accès non autorisé à des serveurs ou à des périphériques réseau | Moyenne | Moyenne | Moyenne | Salles de serveurs sécurisées avec contrôle d'accès |
| | Pannes de courant | Moyenne | Moyenne | Moyenne | Utilisez des parasurtenseurs et des onduleurs<br><br>Envisagez de les héberger dans des centres de données sécurisés approuvés par le gouvernement |

## Annexe 9 : Plan de sauvegarde et de restauration

### 1. Généralités sur la sauvegarde et la restauration

Le chef de l'unité de sécurité du COHIS est responsable de la mise en place et la stratégie des sauvegardes et restaurations du COHIS.

Une bonne gestion des sauvegardes (backups) est essentielle pour assurer la continuité des activités, la protection des données et la résilience face aux incidents (cyber-attaques, pannes, erreurs humaines).

Quelques bonnes pratiques à adopter :

- **ISO 27001 - A.8.13 (sauvegarde de l'information) :** elle exige la mise en place de sauvegardes régulières des informations essentielles. Elle recommande aussi des procédures de sauvegarde bien définies avec des tests réguliers de restauration ;
- **ISO 27001 - A.5.29 / ISO 27002 - A.17.1.2 (mise en œuvre de la continuité) :** nécessite des stratégies de continuité basées sur les sauvegardes ;
- **ISO 27001 - A.5.29 / ISO 27002 - A.17.1.3 (vérification, mise à jour et évaluation des sauvegardes) :** recommande des tests de récupération réguliers pour garantir l'efficacité des sauvegardes.

#### 1.1. Définir une politique de sauvegarde

La première étape consiste à identifier les données critiques à sauvegarder, notamment les bases de données, les fichiers métiers et les configurations systèmes, conformément à la norme ISO 27001 (contrôle A.5.12 relatif à la classification de l'information). Il convient ensuite de déterminer la fréquence des sauvegardes en fonction des besoins opérationnels ; celles-ci peuvent être quotidiennes, hebdomadaires ou en temps réel. Il est également important de fixer une durée de rétention des sauvegardes, par exemple en conservant les copies pendant une période allant de trois à six mois.

#### 1.2. Sécuriser les sauvegardes

La sécurité des sauvegardes est essentielle pour prévenir tout accès non autorisé. Cela passe par le chiffrement systématique des fichiers de sauvegarde, en conformité avec les exigences des contrôles A.8.24 de l'ISO 27001 et A.10.1.1 de l'ISO 27002, qui concernent la politique de cryptographie. L'accès à ces sauvegardes doit être strictement limité aux personnes habilitées, tel que le recommande le contrôle A.8.3 de l'ISO 27001. Par ailleurs, il est essentiel de protéger les sauvegardes contre les attaques de type ransomware, notamment en utilisant des supports de stockage immuables, comme le recommande le contrôle A.8.13.

#### 1.3. Automatiser et tester régulièrement les sauvegardes

Pour éviter les erreurs humaines ou les oublis, il est recommandé de mettre en place un système de sauvegarde automatisé. Il est également indispensable de procéder à des tests réguliers de restauration, afin de vérifier que les sauvegardes sont bien exploitables en cas de sinistre. Ces pratiques sont encadrées par les contrôles A.5.29 de l'ISO 27001 et A.17.1.3 de l'ISO 27002.

### 1.4. Vérifier la qualité des backups et contrôler la restauration

Une sauvegarde n'a de valeur que si elle peut être restaurée avec succès. Il est donc fondamental d'effectuer des tests de restauration périodiques pour vérifier que les données sauvegardées sont complètes, cohérentes et fonctionnelles, conformément aux exigences des contrôles A.5.29 de l'ISO 27001 et A.17.1.3 de l'ISO 27002. L'intégrité des fichiers restaurés doit être contrôlée en les comparant aux données d'origine. Enfin, des rapports de contrôle doivent être mis en place pour assurer le suivi de la qualité des sauvegardes et détecter toute erreur ou défaillance.

### 1.5. Utiliser une solution de sauvegarde adaptée

Le choix de la solution de sauvegarde doit tenir compte du volume et de la criticité des données. Il peut s'agir d'une solution locale, cloud ou hybride. Il est également crucial de vérifier la rapidité de restauration offerte par la solution choisie, afin de minimiser l'impact sur l'activité en cas d'incident.

En résumé, une politique de sauvegarde efficace ne se limite pas à la simple duplication des données. Elle doit inclure des mesures strictes de sécurité, une automatisation fiable, une capacité de restauration testée et des contrôles de qualité rigoureux, le tout en conformité avec les exigences des normes ISO 27001 et 27002.

## 2. Sauvegarde des données du COHIS

### 2.1. Principes directeurs

Nous utiliserons le principe du 3-2-1. Le principe du 3-2-1 est une règle fondamentale en matière de sauvegarde des données. Il vise à garantir une résilience maximale face aux pertes de données, aux incidents techniques ou aux attaques (comme les ransomwares). Ce principe repose sur trois recommandations simples et robustes :

- Trois (03) copies des données (1 originale + 2 copies) ;
- Deux (02) types de stockage différents (ex.: disque dur local + cloud). (ISO 27001 - A.8.13) ;
- Une (01) copie hors site (ex.: serveur distant ou stockage cloud sécurisé).

Il faut conserver au moins trois copies de ces données: cela comprend la copie principale (les données de production) et deux copies de sauvegarde. L'objectif est de réduire le risque de perte totale si une copie est corrompue ou inaccessible. Ces copies doivent être stockées sur au moins deux supports différents. Par exemple, une copie peut être sur un disque dur interne, une autre sur un NAS ou un disque externe, ou encore sur un serveur distant. L'utilisation de supports variés permet de limiter l'impact en cas de défaillance physique ou logicielle d'un support unique. Enfin, au moins une de ces copies doit être conservée hors site (off-site). Cela signifie qu'elle doit être stockée dans un lieu différent de celui où se trouvent les données d'origine, comme dans un autre bâtiment, un centre de données sécurisé, ou dans le cloud. Cette précaution permet de protéger les données même en cas de sinistre local (incendie, inondation, vol, etc.).

En résumé, le principe 3-2-1 garantit la disponibilité et la sécurité des données même dans les situations les plus critiques.

### 2.2. Typologie des sauvegardes

Pour des raisons d'efficacité à la restauration nous utilisons la sauvegarde complète (Full backup). Il existe trois principaux types de sauvegardes utilisés dans les systèmes d'information comme le COHIS, chacun ayant des caractéristiques spécifiques en termes de contenu, de fréquence et de stratégie de restauration :

- **Sauvegarde complète (Full Backup) :**
  - Description : copie intégrale des données ;
  - Fréquence : hebdomadaire (ex. chaque dimanche à 2h).
- **Sauvegarde incrémentale :**
  - Description : ne sauvegarde que ce qui a changé depuis la dernière sauvegarde ;
  - Fréquence : quotidienne (ex. tous les soirs à 22h).
- **Sauvegarde différée :**
  - Description : sauvegarde des changements depuis la dernière sauvegarde complète ;
  - Fréquence : alternative à l'incrémentale si mieux adaptée au volume.

**La sauvegarde complète (ou full backup)** consiste en une copie intégrale de toutes les données ciblées. Elle constitue la base de toute stratégie de sauvegarde, car elle permet de restaurer entièrement un système à un instant donné, sans dépendre d'autres sauvegardes intermédiaires. Ce type de sauvegarde est généralement effectué de façon hebdomadaire, par exemple chaque dimanche à 2 heures du matin, afin de capter l'ensemble des fichiers dans un état cohérent.

**La sauvegarde incrémentale** est une méthode plus optimisée en termes de volume de données à stocker et de rapidité d'exécution. Elle ne copie que les fichiers ou les blocs de données ayant été modifiés depuis la dernière sauvegarde (qu'elle soit complète ou incrémentale). Cette méthode est souvent utilisée quotidiennement, par exemple chaque soir à 22 heures, pour compléter la sauvegarde hebdomadaire sans dupliquer inutilement les données inchangées.

Enfin, la **sauvegarde différentielle** enregistre l'ensemble des changements effectués depuis la dernière sauvegarde complète, sans tenir compte des sauvegardes incrémentales intermédiaires. Cette méthode peut être utilisée comme alternative à la sauvegarde incrémentale, notamment lorsqu'on souhaite un compromis entre la rapidité de sauvegarde et la simplicité de restauration. Elle est souvent choisie lorsque le volume de données change peu entre les cycles ou lorsque le système exige une restauration plus rapide que celle permise par une chaîne de sauvegardes incrémentales.

Ces trois types de sauvegarde sont complémentaires et peuvent être combinés selon les besoins de sécurité, de performance et de disponibilité des données du système.

### 2.3. Propositions d'emplacements et supports de sauvegarde

Le choix des emplacements et supports de sauvegarde est essentiel pour garantir la sécurité et la disponibilité des données.

| Type de support | Usage | Exemple |
|---|---|---|
| Serveur local | Restauration rapide | NAS dans la salle serveur |
| Disque externe chiffré | Copie manuelle ou automatique | Copie hebdo déplacée hors site |
| Cloud sécurisé | Réplication automatique | CAMTEL, CAMPOST, ORANGE, MTN |

### 2.4. Plan de rétention

Le plan de rétention prévoit une politique d'effacement automatique pour éviter l'encombrement, via un script journalisé.

| Type de sauvegarde | Fréquence | Durée de conservation |
|---|---|---|
| Journalière | Tous les jours | Conserver 7 jours |
| Hebdomadaire | 1 par semaine | Conserver 4 semaines |
| Mensuelle | 1 par mois | Conserver 6 mois |
| Annuelle | 1 par an (archivage légal) | Conserver 5 à 10 ans |

## 3. Plan de restauration des données du COHIS

### 3.1. Principes directeurs

- Types de restauration :
  - Restauration partielle par exemple, un fichier corrompu ;
  - Restauration totale par exemple, serveur compromis ou sinistre physique.
- Objectifs de temps de reprise (RTO/RPO) :
  - RTO ≤ 24h pour les données critiques ;
  - RTO ≤ 3 jours pour les données importantes ;
  - RTO ≤ 7 jours pour les données moins sensibles ;
  - Objectif de Point de Reprise (Recovery Point Objective): perte maximale de 7 jours de données (idéalement moins).
- Procédure étape par étape :
  1. Identifier la cause de l'incident ;
  2. Notifier les parties prenantes ;
  3. Identifier le jeu de sauvegarde adéquat ;
  4. Restaurer dans un environnement isolé (test) ;

5. Restauration finale + vérification d'intégrité ;
6. Remplissage de la fiche d'intervention (rapport d'incident).

- Tests réguliers : Il est recommandé de maintenir les équipes techniques et opérationnelles en procédant à :
  - un test trimestriel : pour le test de restauration partielle des données perdues ;
  - un test semestriel : pour la simulation de perte complète des données.

Au cours des tests, il est important d'effectuer le suivi et reporting en documentant :

- Le journal des tests avec : date, durée, succès/échec, remarques ;
- Le rapport annuel est soumis au Comité d'Orientation Stratégique.

### 3.2. Procédures opérationnelles standardisées (POS) relatives à la sauvegarde et à la restauration

- **La sécurité des sauvegardes**

La sécurité des sauvegardes vise à protéger les données contre toute perte, altération ou accès non autorisé.

| Notion | POS |
|---|---|
| **Le chiffrement** | Toujours chiffrer les backups via des chiffrements réputés (AES-256 par exemple) |
| **Qui a accès aux sauvegardes** | - Restreindre les droits d'accès physiques et numériques aux sauvegardes uniquement à la cellule informatique du MINSANTE ;<br>- Journaliser systématiquement les restaurations (qui, quand, pourquoi). |
| **Sauvegardes immuables** | Utiliser les systèmes à verrouillage d'écriture pour éviter la suppression des backups |

- **Plan de Continuité et de Reprise d'Activité (PCA / PRA)**

Le principal objectif d'un PCA/PRA c'est d'assurer la continuité des services critiques en cas d'incident. Ci-dessous, quelques scénarios illustrant comment assurer le PRA :

| Scénario | Impact | Solution PCA | Solution PRA |
|---|---|---|---|
| **Cyberattaque** | Systèmes paralysés | Bascule sur infra secondaire | Restauration full à J-1 |
| **Panne serveur** | Appli injoignable | Accès via serveur de secours | Réinstallation complète |
| **Sinistre local (incendie, inondation...)** | Perte des équipements | VM de secours dans un cloud | Restauration depuis copie hors site |
| **Erreur humaine (suppression)** | Suppression accidentelle | Restauration partielle rapide | Journalisation + validation multi-niveaux |

Pour le PCA, les astuces suivantes permettent d'assurer la reprise en cas d'incident :

- Prévoir un site secondaire (physique ou distant) capable d'héberger les applications critiques ;
- Synchroniser régulièrement les bases de données ;
- Développer des Scripts pour le redéploiement rapide des machines virtuelles/microservices (ou procédure manuelle de lancement des services).

Certaines bonnes pratiques doivent être mises en place pour assurer l'efficacité et la fiabilité des sauvegardes :

- Définir les modèles de rapports de sauvegarde ;
- Dresser une checklist des tests de restauration ;
- Etablir la liste des données critiques par projets ;
- Rendre public et accessible la liste des contacts d'urgence (CI-MINSANTE, PNPLZER, …).

## Annexe 10 : Procédure de gestion des comptes.

### 1. Objectif

La politique de gestion des comptes définit les règles et procédures encadrant la création, l'attribution, la modification, la suspension et la suppression des comptes utilisateurs ayant accès à la plateforme COHIS et à ses ressources partagées entre ministères sectoriels, elle a pour objectif :

- Identifier les utilisateurs ;
- Empêcher tout accès non autorisé aux données ;
- Garantir que chaque compte est justifié, traçable et maîtrisé ;
- Réduire la surface d'attaque en éliminant les comptes dormants ou obsolètes ;
- Assurer la traçabilité complète des activités des utilisateurs.

### 2. Procédures

- **Création de compte :** la création d'un compte doit obligatoirement suivre une procédure formelle, reposant sur une demande écrite ou via un formulaire électronique, et précisant le rôle à attribuer (ex. lecteur, éditeur, administrateur, super-administrateur). Les comptes sont strictement individuels et ne peuvent en aucun cas être partagés entre plusieurs utilisateurs. Un formulaire standard de demande de création de compte COHIS est prévu à cet effet (voir ci-dessous). Il est également proposé de mettre en place un formulaire en ligne permettant aux utilisateurs de soumettre directement leur demande de création de compte ;
- **Gestion des rôles et privilèges :** l'attribution des droits d'accès est régie par le principe du moindre privilège (*Least Privilege Principle*). Ainsi, chaque utilisateur se voit conférer uniquement les autorisations strictement nécessaires à l'exercice de ses fonctions ;
- **Authentification forte :** il est institué la mise en place d'un mécanisme d'authentification multifactorielle (MFA), applicable à l'ensemble des comptes administrateurs, et ce, dans la mesure du possible ;
- **Durée de vie des comptes** : les comptes temporaires, tels que ceux attribués aux consultants, doivent être créés avec une date d'expiration prédéfinie afin d'en limiter la validité. Quant aux comptes permanents, ils doivent faire l'objet d'une revue annuelle obligatoire, visant à confirmer la légitimité des accès accordés et à garantir leur conformité avec les fonctions effectivement exercées par les utilisateurs ;
- **Limitation des tentatives d'accès :** les comptes utilisateurs doivent être configurés pour restreindre le nombre de tentatives de connexion. Lorsqu'une limite prédéfinie est atteinte, l'accès au compte doit être temporairement ou définitivement bloqué afin de prévenir toute tentative d'intrusion ;
- **Révision périodique des accès et des habilitations :** les administrations sectorielles doivent effectuer une revue trimestrielle des comptes et droits associés ;

- **Gestion des comptes inactifs :** tout compte utilisateur faisant l'objet d'une inactivité prolongée est automatiquement suspendu après une période prédéfinie. En cas de non-utilisation persistante, telle qu'une durée excédant six (0 6) mois, le compte est définitivement supprimé. Par ailleurs, les droits d'accès sont systématiquement réalignés afin de demeurer en adéquation avec les fonctions effectivement exercées par l'utilisateur ;
- **Journalisation des activités :** toutes les actions sensibles (connexion, modification, exportation) sont enregistrées et associées à un compte utilisateur identifié ;
- **Réinitialisation sécurisée :** une procédure sécurisée est définie pour la réinitialisation de mots de passe, incluant la vérification d'identité et des canaux chiffrés ;
- **Clôture de compte :** lorsqu'un utilisateur quitte un ministère ou change de fonction, son compte doit être désactivé immédiatement, puis supprimé dans les 30 jours ;
- **Politique de mot de passe :** tout mot de passe doit comporter une longueur minimale de douze (12) caractères, incluant obligatoirement des majuscules, des minuscules, des chiffres ainsi que des caractères spéciaux, afin d'assurer un niveau de complexité suffisant. La durée de validité d'un mot de passe est fixée à six (06) mois maximum, au terme desquels il doit être renouvelé. Par ailleurs, tout utilisateur est tenu de modifier son mot de passe dès sa première connexion lorsqu'il lui a été attribué automatiquement ou par un administrateur, que ce soit lors de la création du compte ou lors d'un renouvellement. Enfin, les mots de passe ne doivent en aucun cas être conservés en clair ; ils doivent obligatoirement être protégés par un algorithme de chiffrement ou de hachage robuste avant leur stockage.

## 3. Formulaire de demande de création de compte COHIS

### A. Informations générales du demandeur

- Nom complet : .....
- Fonction / Poste occupé : .....
- Ministère / Institution : .....
- Service / Direction : .....
- Adresse email professionnelle : .....
- Téléphone professionnel : .....

### B. Type de compte demandé

- ☐ Producteur des données
- ☐ Intendant des données
- ☐ Administrateur du système
- ☐ Analyste / Visualisation

- ☐ Consommateur des données
- ☐ Autre : .....

**C. Justification de la Demande : objectif d'utilisation du COHIS :**

.....
.....

**D. Engagement de l'Utilisateur**

Je m'engage à utiliser mon compte COHIS dans le strict respect des politiques de sécurité, de confidentialité et de gouvernance des données définies par la Plateforme *One Health*. Je comprends que toute utilisation abusive peut entraîner la suspension ou la révocation de mon accès. Joindre la fiche d'accord d'utilisation de COHIS.

**E. Pour usage interne (intendants des données du COHIS)**

- **Date de réception:** ____ / ____ / _____
- **Décision :** ☐ Approuvée ☐ Rejetée
- **Compte créé par :** .....
- **Date d'activation :** ____ / ____ / _____
- **Observations :** .....

MM

## Annexe 11 : Contrôles des personnes.

Le contrôle des personnes dans un premier temps vise à sensibiliser les utilisateurs à la sécurité. En effet, même dans un système à niveau de sécurité techniquement sécurisé, l'erreur humaine ou la mauvaise utilisation présente souvent le risque le plus élevé. Ces contrôles définissent les procédures d'intégration des utilisateurs, telles que l'obligation de prendre connaissance et de signer une note de confidentialité des données, ainsi que les processus de gestion des comptes et des droits d'accès. Ils incluent également les mesures de formation et de sensibilisation, afin de s'assurer que chaque utilisateur comprend et respecte les dispositifs de protection des données et de sécurité de l'information. Enfin, lorsque les utilisateurs accèdent au système avec leurs propres appareils, le contrôle d'accès de ces dispositifs doit être assuré par le biais des mesures de contrôle des personnes, garantissant ainsi la sécurité globale du système.

### 1. Procédure de Contrôles des Personnes

| Procédure | Description dans le contexte COHIS |
|---|---|
| **Contrôle préalable à l'accès** | Avant de pouvoir accéder à COHIS, tout utilisateur doit être enregistré dans une base officielle, validé par sa hiérarchie et attribué à un rôle spécifique conformément au mécanisme RBAC (Role-Based Access Control). |
| **Enregistrement et habilitation des utilisateurs** | Chaque ministère doit tenir un registre des utilisateurs habilités à accéder à COHIS, précisant: nom, matricule, fonction, niveau d'accès, date d'attribution, durée de validité, responsable hiérarchique. |
| **Revue régulière des accès** | Tous les trimestres, une revue des comptes utilisateurs est effectuée: comptes inactifs, droits excessifs, utilisateurs mutés, sortants… Toute anomalie entraîne suspension ou suppression du compte. |
| **Sensibilisation obligatoire avant accès** | Tout agent doit suivre une formation de base à la sécurité COHIS avant d'obtenir un compte, incluant: protection des identifiants, règles de partage, comportement en cas d'incident. |
| **Politique d'utilisation acceptable (PUA)** | Chaque utilisateur doit signer une charte d'usage précisant ce qui est autorisé ou interdit sur COHIS (ex.: interdiction de partager ses identifiants, usage personnel interdit, signalement d'anomalie obligatoire). |
| **Contrôle d'identité à la connexion** | Implémentation d'une authentification forte (ex.: mot de passe + code OTP via mobile) pour s'assurer que la personne accédant à COHIS est bien celle autorisée. |
| **Traçabilité des actions** | Chaque action sensible d'un utilisateur sur COHIS (ex: téléchargement de données, modification, suppression, consultation de données sensibles) est journalisée et associée à son identité. |
| **Réponse comportementale** | Mise en place d'un système de détection de comportements anormaux (ex.: connexions à des heures inhabituelles, consultation |

| | |
|---|---|
| | massive de fichiers). En cas d'alerte, l'accès peut être suspendu en urgence. |
| **Procédure de sortie** | Lorsqu'un agent quitte son poste ou est muté, son compte doit être désactivé immédiatement et ses droits révoqués. Un audit post-sortie peut être fait pour vérifier ses dernières actions. |
| **Audit interne et contrôle croisé** | Chaque ministère audite ses propres accès et peut être audité par COHIS pour s'assurer que ses utilisateurs respectent les règles de sécurité. |

## 2. Plan de sensibilisation et de formation des utilisateurs

La sensibilisation et la formation des utilisateurs de la plateforme COHIS est un levier majeur de sécurité organisationnelle selon les normes ISO/IEC 27001, 27002, 27005 car l'humain est souvent le maillon le plus vulnérable dans la chaîne de sécurité.

Ce plan a pour objectif de sensibiliser, former, responsabiliser et impliquer les utilisateurs sur les bonnes pratiques de sécurité numérique, les risques liés à l'utilisation de COHIS et les réflexes à adopter pour prévenir les incidents ou y répondre.

### 2.1. Identification des profils à former

- Utilisateurs de la plateforme COHIS (producteurs, intendant de données et administrateurs) ;
- Personnel IT ou responsables locaux de la sécurité informatique (RSSI, points focaux SSI) ;
- Responsables de la gouvernance des données ;
- Prestataires ou consultants ayant accès à COHIS ;

Un registre des utilisateurs avec rôle et niveau de responsabilité est nécessaire pour adapter les formations.

### 2.2. Définition des contenus pédagogiques par profil

- Pour les utilisateurs finaux :
    - Comprendre les types de données sensibles ;
    - Bonnes pratiques de mot de passe ;
    - Reconnaître un e-mail de phishing ;
    - Sécurité physique des appareils ;
    - Règles d'accès à COHIS et signalement d'incident.
- Pour les responsables techniques :
    - Configuration sécurisée ;
    - Gestion des journaux et des accès ;
    - Sauvegarde/restauration ;

  - Résolution d'incidents ;
  - Conformité ISO/IEC.
- Pour les responsables de gouvernances des données :
  - Gouvernance des données ;
  - Risques organisationnels ;
  - Obligations légales ;
  - Lecture d'un rapport de sécurité.

### 2.3. Choix des formats de formation

- Sessions présentielles dans chaque ministère au moins 1 fois par an ;
- Modules e-learning accessibles via un portail sécurisé (plateforme COHIS ou LMS) ;
- Simulations d'attaque (phishing, réponse à incident) ;
- Diffusion de bulletins périodiques ou infographies pédagogiques ;
- Quiz de validation des acquis.

### 2.4. Planification annuelle

- Élaboration d'un calendrier de sensibilisation coordonné entre la cellule sécurité de COHIS et les référents de chaque ministère ;
- Obligation de participation selon les postes critiques.

### 2.5. Mise en œuvre et traçabilité

- Enregistrement des présences en formation ;
- Signature d'engagement de confidentialité à l'issue de chaque session ;
- Génération d'un certificat de sensibilisation (utile lors d'audits) ;
- Intégration dans le dossier RH de l'agent.

### 2.6. Évaluation de l'efficacité

- Évaluations à chaud : questionnaire post-formation ;
- Évaluations à froid : tests réels (phishing simulé, audit surprise) ;
- Analyse des incidences post-formations (réduction ou non).

### 2.7. Mise à jour continue des contenus

- Adapter les formations à l'évolution des menaces ;
- Prendre en compte les nouveaux modules fonctionnels de COHIS ;
- Réviser après chaque audit ou incident significatif.

## Annexe 12 : Processus de mise à disposition des données au public.

### 1. Définition

La mise à disposition des données au public désigne l'ensemble des étapes permettant à un ministère sectoriel, via COHIS, de publier ou partager des jeux de données au grand public (journalistes, étudiants, chercheurs, partenaires internationaux, etc.).

### 2. Enjeux critiques

- Conformité légale : respecter les lois camerounaises sur la protection des données, la transparence administrative et les éventuelles directives de l'Union Africaine (UA) ;
- Protection des données sensibles : éviter toute fuite d'informations à caractère personnel ou stratégique ;
- Cohérence et contrôle : s'assurer que les données sont à jour, validées, et diffusées selon un processus approuvé et traçable ;
- Responsabilité: pouvoir identifier clairement qui a autorisé la publication, à quel moment, sous quelles conditions, et dans quel format.

### 3. Processus de mise à disposition des données via COHIS - Voici les étapes clés à intégrer dans un processus sécurisé

#### 3.1. Demande d'intention de publication

Le ministère sectoriel producteur identifie un jeu de données à partager publiquement. Il remplit un formulaire d'intention via COHIS précisant :

- Objectif de publication ;
- Public visé ;
- Sensibilité potentielle ;
- Fréquence de mise à jour.

#### 3.2. Classification et évaluation du risque

Les données sont classées selon leur sensibilité (ex.: publique, interne, confidentielle, critique). Un RSSI ou point focal sécurité du ministère sectoriel évalue les risques associés à leur publication (ex. : données de santé, sécurité nationale, etc.).

#### 3.3. Validation par une autorité compétente

La demande est soumise à validation hiérarchique (ex.: Direction générale, cellule juridique, ou comité de gouvernance des données).

Si les données concernent plusieurs ministères sectoriels, la validation conjointe est requise.

#### 3.4. Nettoyage et anonymisation

Avant publication, les données sont :

- Dépersonnalisées si nécessaire (ex.: suppression de noms, adresses) ;
- Agrégées pour éviter une identification indirecte ;
- Vérifiées sur leur exactitude et cohérence ;
- Choix du canal de diffusion.

Les données peuvent être rendues disponibles :

- Sur un portail open data (COHIS ou externe) qui pourrait aussi être accessible via la page du Système National d'Information Statistique (SNIS) sur le site de l'Institut National de la Statistique qui est l'organisme étatique chargé de la coordination du SNIS, afin d'accroître sa visibilité ;
- Via une API publique sécurisée ;
- Sous forme de tableaux de bord ou rapports dynamiques ;
- Traçabilité de la décision.

COHIS journalise :

- Le nom du décideur qui a autorisé la publication ;
- La date de validation ;
- Le contenu exact publié ;
- Les conditions d'accès (ex.: téléchargement libre, demande d'accès, usage non commercial, etc.) ;
- Information au public.

Le jeu de données est accompagné :

- D'une fiche descriptive (métadonnées, source, méthode de collecte, fréquence de mise à jour) ;
- D'un cadre juridique (licence de réutilisation, mention obligatoire de la source) ;
- Suivi post-publication.

COHIS permet de :

- Suivre l'usage des données (téléchargements, utilisateurs) ;
- Recevoir des retours du public (corrections, suggestions) ;
- Déclencher un retrait temporaire ou définitif si un risque est détecté ;
- Exemple de règles de sécurité spécifiques à la mise à disposition publique.

| Exigence | Mécanisme COHIS |
|---|---|
| Ne jamais publier de données à caractère personnel | Filtres automatiques + validation humaine |

| | |
|---|---|
| Assurer que les données sont fiables et à jour | Validation manuelle + horodatage de mise à jour |
| Traçabilité de chaque publication | Historique des publications par ministère et par validateur |
| Usage restreint si nécessaire | Attribution de licences d'utilisation spécifiques via COHIS (ODbL, CC-BY, etc.) |

La mise à disposition des données au public via COHIS n'est pas un simple téléchargement, mais un processus encadré, évalué, validé, tracé et réversible, qui protège à la fois la sécurité nationale, la vie privée, et la crédibilité des institutions publiques.

## Annexe 13 : Gestion des certificats de sécurité.

### 1. Définition

Il s'agit de l'ensemble des processus techniques et organisationnels permettant de créer, délivrer, stocker, renouveler, révoquer et contrôler l'usage des certificats numériques utilisés pour sécuriser les communications, authentifier les serveurs et chiffrer les données échangées sur COHIS.

Ces certificats reposent sur des technologies de chiffrement à clé publique (PKI – Public Key Infrastructure).

### 2. Objectifs de la gestion des certificats dans le contexte COHIS

| Objectifs | Détails |
|---|---|
| **Sécuriser les échanges de données** | Grâce au chiffrement SSL/TLS, les certificats assurent que les données transitent de manière chiffrée entre les ministères. |
| **Authentifier les serveurs COHIS** | Le certificat garantit que le serveur COHIS est bien celui autorisé par l'État, évitant les attaques de type "man-in-the-middle". |
| **Garantir la non-altération des données** | Le certificat participe à la signature électronique de données ou fichiers, ce qui assure qu'ils n'ont pas été modifiés après leur émission. |
| **Prévenir les interruptions de service** | Une bonne gestion évite les certificats expirés, qui peuvent bloquer l'accès à la plateforme. |

### 3. Processus de gestion des certificats pour COHIS

| Étapes | Description dans le contexte COHIS |
|---|---|
| **Demande de certificat** | Le responsable technique COHIS (ou d'un ministère) soumet une demande à une autorité de certification agréée (ex: Agence Nationale de Certification Électronique, PKI Cameroun, ou équivalent approuvé). |
| **Validation d'identité** | L'autorité de certification vérifie l'identité de l'organisation demandeuse (ex: ministère, hébergeur de COHIS) avant d'émettre un certificat. |
| **Émission du certificat** | Le certificat contient : nom du domaine, date de validité, clé publique, nom de l'entité, signature de l'autorité de certification. |
| **Installation sur les serveurs COHIS** | Les certificats sont installés sur les serveurs web, API, ou services d'échange interconnectés (en TLS 1.3). |
| **Surveillance de la validité** | Un outil de monitoring automatique (ex: Cron+OpenSSL, ou solution SIEM) surveille les dates d'expiration. |

| | |
|---|---|
| **Renouvellement anticipé** | Tout certificat doit être renouvelé au moins 15 jours avant expiration, pour éviter une interruption de service. |
| **Révocation si compromission** | En cas de piratage, un certificat peut être révoqué et ajouté à une liste de révocations (CRL). |
| **Journalisation et archivage** | Chaque action liée aux certificats (création, renouvellement, révocation) est consignée dans les journaux de sécurité du COHIS. |

## 4. Types de certificats utilisés dans COHIS

| Type | Utilisation |
|---|---|
| **Certificats SSL/TLS** | Pour chiffrer les échanges entre les navigateurs/ministères et les serveurs du COHIS. |
| **Certificats clients (mutuels)** | Pour authentifier certains utilisateurs ou machines sensibles lors de connexions à des services critiques. |
| **Certificats de signature de code** | Pour signer numériquement les fichiers, scripts ou modules diffusés sur COHIS (garantir l'origine et l'intégrité). |

## 5. Bonnes pratiques à formaliser dans une politique de gestion des certificats

Les bonnes pratiques suivantes doivent être formalisées dans les politiques de gestion des certificats :

- Tenue d'un registre centralisé de tous les certificats utilisés (ministère, type, date d'expiration, usage) ;
- Automatisation des alertes pour éviter les expirations non anticipées ;
- Protection des clés privées associées aux certificats (coffres forts numériques, HSM, permissions strictes) ;
- Utilisation d'une autorité de certification de confiance et centralisée, idéalement gouvernementale ;
- Test régulier des configurations TLS via des outils comme SSL Labs, ou scans internes ;
- Révocation immédiate en cas de compromission ou de changement d'usage.

En résumé, la gestion rigoureuse des certificats de sécurité dans COHIS protège les données échangées, garantit l'authenticité des serveurs, préserve la continuité des services, et s'aligne avec les exigences de l'ISO/IEC 27001 (contrôles techniques A.10.1 et A.18.1).

## Annexe 14 : Surveillance et gestion des risques.

### 1. Objectif

Assurer la détection précoce, la traçabilité, la réponse rapide et l'analyse post-incident de toute situation de sécurité pouvant affecter la disponibilité, l'intégrité ou la confidentialité des données échangées via COHIS.

### 2. Composantes clés de la surveillance et gestion des incidents dans COHIS

#### 2.1. Mise en place d'un système de surveillance centralisé

| Élément | Détail |
|---|---|
| **SIEM (Security Information and Event Management)** | Intégrer un outil (ex: Wazuh, Splunk, Graylog) pour collecter, corréler et analyser en temps réel tous les journaux (logs) système, applicatif, réseau, et bases de données liées à COHIS. |
| **Détection d'anomalies comportementales** | Utiliser des algorithmes pour repérer des comportements inhabituels (ex.: un agent télécharge 100 fichiers à 3h du matin). |
| **Journalisation obligatoire (logs)** | Tous les ministères interconnectés doivent activer la journalisation : connexions, tentatives échouées, accès aux données sensibles, changements critiques. |

#### 2.2. Détection des incidents potentiels

Les incidents de sécurité potentiels peuvent prendre différentes formes et menacer l'intégrité, la disponibilité ou la confidentialité des systèmes d'information. Parmi les plus courants, on retrouve :

- Tentatives d'accès non autorisé ;
- Malware détecté sur un serveur (virus, ransomware, trojan, spyware) ;
- Fuite de données interne (volontaire, négligence, erreur de manipulation) ;
- Déni de service distribué (DDoS) ;
- Altération ou suppression non autorisées de données (intentionnelle ou accidentelle) ;
- Exportation non autorisée de données sensibles ;
- Perte ou vol de supports contenant des données sensibles (ordinateurs portables, disques externes, clés USB).

#### 2.3. Procédure formalisée de gestion des incidents

| Étape | Description dans COHIS |
|---|---|
| **Identification** | Un utilisateur, un système ou un outil SIEM signale un événement suspect. |
| **Classification** | L'événement est classé : alerte, incident mineur, majeur ou critique. |

| | |
|---|---|
| **Enquête rapide** | L'équipe sécurité COHIS, en lien avec le ministère concerné, analyse la cause et l'étendue. |
| **Notification immédiate** | En cas d'impact interinstitutionnel ou critique, notification au Comité de gouvernance de la sécurité du COHIS et, si nécessaire, aux autorités légales. |
| **Réponse et confinement** | Isolement du serveur affecté, désactivation des comptes compromis, blocage temporaire d'accès, restauration à partir des sauvegardes si besoin. |
| **Rétablissement des services** | Reprise contrôlée avec validation de l'intégrité des systèmes. |
| **Rétro-analyse (post-mortem)** | Rapport d'incident détaillé : origine, faille exploitée, impact, mesures correctives immédiates et de long terme. |
| **Capitalisation** | Mise à jour des procédures, formation si l'incident est dû à une erreur humaine, ou renforcement de la politique de sécurité. |

### 2.4. Rôles et responsabilités

| Acteurs | Rôles |
|---|---|
| **Cellule Informatique (CI) du MINSANTE** | Supervise la détection, la coordination des réponses, l'analyse et la documentation. |
| **Référents SSI des sectorielles** | Point de contact local pour toute alerte ou enquête. |
| **PNPLZER et CI MINSANTE** | Reçoit les rapports, approuve les mesures structurelles, assure le suivi politique. |
| **CI MINSANTE** | Renforcent la sensibilisation post-incident. |

### 2.5. Indicateurs de performance (KPI) à suivre

| KPI | Objectif |
|---|---|
| Temps moyen de détection (MTTD) | < 5 minutes |
| Temps moyen de résolution (MTTR) | < 24 heures |
| Nombre d'incidents critiques par trimestre | En diminution |
| Taux d'incidents dus à une erreur humaine | < 15 % |
| Taux de traitement des recommandations post-incident | ≥ 90 % |

### 2.6. Bonnes pratiques complémentaires à COHIS

Afin de renforcer l'efficacité du COHIS et d'assurer une gestion optimale des incidents de sécurité, certaines bonnes pratiques complémentaires doivent être mises en place de manière proactive.

- Tests réguliers de simulation d'incidents (exercices de type "table-top" ou "cyber drill") ;
- Documentation d'un plan de réponse aux incidents (PRI) accessible à tous les responsables SSI ;

- Tableau de classification des niveaux d'alerte (niveau 1 à 4) selon impact/sensibilité ;
- Canal sécurisé pour signalement d'incidents par les utilisateurs (ex: bouton « signaler une anomalie » intégré à COHIS) ;
- Stockage sécurisé des logs, horodatés, non modifiables, consultables uniquement sur autorisation.

En résumé, la surveillance et la gestion des incidents dans COHIS permet de détecter en temps réel toute activité suspecte, réagir rapidement pour limiter les dégâts, documenter chaque événement pour apprentissage et conformité, renforcer la posture de cyber-sécurité à l'échelle ministérielle.

## Annexe 15 : Termes de référence de responsabilités de staff technique de PNPLZER.

### 1. Contexte

Le *Cameroon One Health Information System* (COHIS) est une plateforme nationale d'intégration de données conçue pour soutenir la collaboration multisectorielle entre les secteurs de la santé humaine, animale, végétale et environnementale. La plateforme permet le partage de données, l'interopérabilité et la prise de décision fondée sur des preuves, alignées sur les lois camerounaises et les normes internationales, telles que :

#### 1.1. Normes et stratégies internationales :

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;
- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;

- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité.

**1.2. Lois et actes du Cameroun :**

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

## 2. Responsabilités du staff technique du PNPLZER

Le staff technique du PNPLZER joue un rôle central dans la gouvernance opérationnelle des données. Il constitue le pilier technique et méthodologique chargé de soutenir et superviser les intendants de données dans l'application cohérente des principes de gestion des données au sein de la plateforme. Son rôle est multidimensionnel et s'articule autour des missions suivantes :

- **Coordination du traitement des données :** le staff technique du PNPLZER supervise l'ensemble du cycle de vie des données – de l'ingestion à la diffusion – en désignant une équipe multisectorielle pour veiller à l'harmonisation des pratiques entre les différents secteurs (santé humaine, animale, végétale et environnementale). Il facilite la collaboration entre les sectorielles pour garantir une gestion fluide et concertée. Il désigne une équipe multisectorielle ;
- **Assurance qualité et conformité :** le staff technique du PNPLZER veille à la conformité du système aux normes nationales et internationales en matière de qualité des données, notamment la norme ISO 8000. Il s'assure également du respect rigoureux

des processus définis dans les politiques de gestion des données du COHIS. Dans ce cadre il maintient le registre des métadonnées, assure que chaque jeu de données est listé dans le catalogue des jeux des données et archive les fiches de description des données ;

- **Élaboration du plan de gestion des données :** le staff technique du PNPLZER est responsable de la rédaction, de la mise à jour et du suivi du plan de gestion des données, document stratégique décrivant comment les données sont chargées, stockées, documentées, sécurisées, partagées et archivées ;
- **Définition des normes de présentation des données : afin** d'assurer une communication claire et uniforme, le staff technique du PNPLZER établit des standards de visualisation et de présentation des données applicables à l'ensemble des tableaux de bord, rapports, et publications de la plateforme COHIS ;
- **Gestion technique et comptes utilisateurs :** le staff technique du PNPLZER autorise la création, la suspension, la réhabilitation ou la suppression des comptes utilisateurs de la plateforme COHIS ;
- **Responsabilité de l'environnement de partage des données :** le staff technique du PNPLZER conçoit et gère l'environnement de partage sécurisé des données, favorisant l'accès contrôlé à des jeux de données pertinents entre les parties prenantes, selon des protocoles établis ;
- **Plan de formation :** le staff technique du PNPLZER conçoit et met en œuvre un plan de formation continu à destination des utilisateurs, des gestionnaires et des stewards, pour renforcer les compétences en traitement, gouvernance, éthique et valorisation des données ;
- **Veille informationnelle :** en lien avec les besoins stratégiques du *One Health*, le staff technique du PNPLZER effectue une veille informationnelle active sur les meilleures pratiques, outils, normes émergentes et innovations en gestion de données ;
- **Ambassadeur de la culture de la donnée :** le staff technique du PNPLZER agit comme ambassadeur de la donnée, promouvant une culture organisationnelle qui repose sur la prise de décision basée sur les données probantes. Il participe à la valorisation des données à travers la communication, les événements et la mobilisation des partenaires ;
- **Suivi et évaluation de la gestion des données :** enfin, le staff technique du PNPLZER met en place un système de suivi-évaluation permettant de mesurer la maturité de la gestion des données, identifier les écarts, et proposer des actions correctives et des axes d'amélioration continue.

## Annexe 16 : Termes de référence de responsabilités de staff technique de la Cellule Informatique du MINSANTE.

### 1. Contexte

Le *Cameroon One Health Information System* (COHIS) est une plateforme nationale d'intégration de données conçue pour soutenir la collaboration multisectorielle entre les secteurs de la santé humaine, animale, végétale et environnementale. La plateforme permet le partage de données, l'interopérabilité et la prise de décision fondée sur des preuves, alignées sur les lois camerounaises et les normes internationales, telles que :

#### 1.1. Normes et stratégies internationales :

- Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'Intelligence Artificielle (IA) : elle a pour objectif de guider le développement, le déploiement et l'utilisation de l'IA dans le respect des droits humains, de la dignité humaine, de l'inclusion, de la paix, de la justice sociale et du développement durable ;
- Cadre Stratégique de l'Union Africaine (UA) en matière de données : il vise à orienter les Etats membres et les institutions continentales dans la gestion, la gouvernance, l'utilisation et la valorisation des données au service du développement durable, de l'intégration régionale et de la transformation numérique ;
- L'initiative de politique et de régulation pour l'Afrique numérique (PRIDA) : c'est une initiative conjointe de l'Union Africaine (UA), de l'Union Européenne (UE), et l'Union Internationale des Télécommunications (UIT) pour harmoniser les politiques et les cadres réglementaires numériques à travers l'Afrique, tout en renforçant les capacités, institutionnelles et humaines des Etats membres pour accompagner la transformation numérique du continent ;
- ISO 8000 (Qualité des données) : elle garantit la qualité, l'échange, l'intégrité et la traçabilité des données, en particulier dans les chaînes logistiques, systèmes d'information et les échanges entre partenaires ;
- ISO/IEC 11179 (Registre de métadonnées) : il définit un cadre pour créer et gérer des registres de métadonnées permettant d'assurer une compréhension commune des données ;
- ISO/IEC 27001 (Système de Management de la Sécurité de l'Information) : c'est une norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI) ;
- ISO/IEC 27002 (Mesures de Sécurité de l'information) : c'est une norme complémentaire à ISO/IEC 27001, un code de bonnes pratiques pour la gestion de la sécurité de l'information qui fournit des lignes directrices détaillées pour la mise en œuvre des mesures de sécurité (aussi appelées Contrôles) ;
- ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information) : c'est une norme qui fournit des lignes directrices pour l'établissement et la mise en œuvre d'un processus

de gestion des risques. Elle aide les organisations à identifier, évaluer, analyser et traiter les risques de sécurité de l'information de manière systématique ;

- Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles (Convention de MALABO) : entrée en vigueur le 06 octobre 2023, ratifiée par le Cameroun, elle introduit un cadre régional harmonisé pour la cybersécurité, la protection des données et la lutte contre la cybercriminalité ;

### 1.2. Lois et actes du Cameroun :

- Loi n°2024/017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun : elle s'applique à tout traitement de données personnelles (automatisé ou non) effectué au Cameroun ou à des personnes y résidant, opérant dans le pays ou visées par la loi. Elle stipule que toute collecte ou traitement doit recevoir une autorisation de l'autorité de protection des données ;
- Loi n°2020/010 du 20 juillet 2020 régissant l'activité statistique au Cameroun : elle garantit la transparence, l'objectivité et l'impartialité dans la production des statistiques. Elle assure aussi une protection des données individuelles via le secret statistique, sous peine de sanctions pénales et administratives ;
- Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité : c'est un cadre juridique pour la sécurité des réseaux et système d'information. Il définit plusieurs infractions et sanctions pénales pour traitements illicites des données personnelles : interception, détention, divulgation, conservation abusive ;
- Loi n°2010/013 du 21 décembre 2010 régissant le commerce électronique au Cameroun : elle encadre les transactions en ligne, la conservation des données et la responsabilité des prestataires électroniques ;
- Loi n°2010/021 du 21 décembre 2010 régissant la communication électronique au Cameroun : elle réglemente les activités des opérateurs et impose des obligations liées à la qualité de service, à la sécurité des réseaux et au respect des données des abonnés.

## 2. Responsabilité de la Cellule Informatique du MINSANTE

Le staff technique de la Cellule Informatique du MINSANTE est responsable de garantir l'intégrité, la confidentialité et la disponibilité des données et des composantes de la plateforme COHIS. Il constitue le garant de la cybersécurité et de la conformité réglementaire, en assurant une protection continue contre les menaces internes et externes. Ses responsabilités s'articulent autour des axes suivants :

- **Coordination de la sécurité des données de la plateforme :** le staff technique de la Cellule Informatique du MINSANTE supervise l'ensemble des activités liées à la sécurité de l'information au sein du COHIS. Elle coordonne les efforts intersectoriels pour assurer une gestion sécurisée des données et veille à l'application des politiques de sécurité à tous les niveaux du système ;

- **Conformité aux standards de sécurité nationaux et internationaux :** le staff technique de la Cellule Informatique du MINSANTE veille à ce que la plateforme COHIS respecte les normes internationales telles que ISO/IEC 27001, 27002 et 27005 ainsi que les exigences réglementaires nationales applicables en matière de cybersécurité, de protection des données personnelles et de souveraineté numérique ;
- **Respect des normes et réglementations en vigueur :** le staff technique de la Cellule Informatique du MINSANTE suit de près l'évolution des textes législatifs, normes techniques et obligations contractuelles, et intègre ces exigences dans la politique et les procédures de sécurité de la plateforme ;
- **Documentation des procédures de sécurité :** le staff technique de la Cellule Informatique du MINSANTE veille à ce que toutes les procédures opérationnelles liées à la sécurité soient formalisées, documentées, mises à jour et communiquées de manière à garantir la traçabilité, la reproductibilité et l'auditabilité des actions de sécurité ;
- **Élaboration de la politique de sécurité du COHIS :** le staff technique de la Cellule Informatique du MINSANTE rédige, maintient et fait appliquer la politique de sécurité de l'information de la plateforme, qui couvre les aspects organisationnels, techniques, physiques et humains de la cybersécurité, en conformité avec les meilleures pratiques internationales ;
- **Gestion des incidents et reprise d'activité :** le staff technique de la Cellule Informatique du MINSANTE définit les procédures de gestion des incidents de sécurité, de sauvegarde régulière des données, et élabore des plans de continuité et de reprise d'activité (PRA/PCA) pour garantir la résilience opérationnelle de la plateforme en cas de sinistre ou de cyberattaque ;
- **Hébergement sécurisé et administration des serveurs :** le staff technique de la cellule Informatique du MINSANTE assure directement ou via des prestataires de confiance l'hébergement sécurisé de la plateforme, incluant l'administration des serveurs, la surveillance de leur fonctionnement, la mise à jour régulière des logiciels, et la gestion des accès techniques ;
- **Veille sécuritaire et prospective technologique :** le staff technique de la Cellule Informatique du MINSANTE conduit une veille permanente sur les menaces émergentes, les vulnérabilités critiques, et les nouvelles technologies de cybersécurité. Cette veille guide les décisions sur les migrations vers des solutions plus sûres, plus robustes ou plus performantes ;
- **Gestion des comptes des utilisateurs :** le staff technique de la Cellule Informatique du MINSANTE gère le cycle de vie des comptes utilisateurs du COHIS, y compris la création de comptes, les autorisations d'accès, la désactivation et les révisions périodiques. Elle assure que tous les utilisateurs signent les termes d'utilisation du COHIS et elle les archive, intervient en cas d'infraction et les reporte au responsable de la gouvernance des données ;
- **Sensibilisation aux bonnes pratiques de sécurité :** le staff technique de la Cellule Informatique du MINSANTE joue un rôle de formation et de sensibilisation auprès de

tous les acteurs du COHIS (administrateurs, utilisateurs, partenaires) pour promouvoir une culture de cybersécurité, incluant la gestion des mots de passe, la prévention du phishing, la protection des postes de travail, etc.

## Annexe 17 : Plan de financement prévisionnel de fonctionnement de la plateforme COHIS (2026-2028).

| | | 2026 | | | | 2027 | | | | 2028 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Activités** | **T1** | **T2** | **T 3** | **4ème trimestre** | **T 1** | **T 2** | **T 3** | **4ème trimestre** | **T 1** | **T 2** | **T 3** | **4ème trimestre** | **Budget** |
| **Administration et développement du système** | | | | | | | | | | | | | | **250 000 000 XAF** |
| **Hosting/serveurs** | 1. Serveur de production : 16 cœurs, 64 Go de RAM, 2 To de SSD ; 2. Serveur de Propagation : 8 cœurs, 32 Go de RAM ; 1 To de disque SSD ; Serveur de Monitoring : 4 cœurs ; 16 Go de RAM, 500 Go de RAM | | | | | | | | | | | | | **60 000 000 XAF** |
| **Maintenance logicielle** | Installer des correctifs de sécurité/mises à jour du système ; redéployer le système en cas de panne du | | | | | | | | | | | | | **40 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | serveur ; maintenir les performances du système ; tenir à jour la base de données et les comptes d'utilisateurs. | | | | | | | | | | | | | |
| **Développement de logiciels** | Ajouter de nouvelles fonctions, migrer vers une nouvelle version | | | | | | | | | | | | | **120 000 000 XAF** |
| **Formation des administrateurs système** | Formation sur le suivi de la performance du système, le redéploiement du système, le maintien de la performance - 8 administrateurs | | | | | | | | | | | | | **30 000 000 XAF** |
| **Gestion opérationnelle** | | | | | | | | | | | | | | **135 000 000 XAF** |
| **Gestion globale** | Bureaux, internet, | | | | | | | | | | | | | **45 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | personnel, formation | | | | | | | | | | | | | |
| **Unité de sécurité des données** | Bureaux, internet, personnel, formation | | | | | | | | | | | | | **45 000 000 XAF** |
| **Unité de traitement des données** | Bureaux, internet, personnel, formation | | | | | | | | | | | | | **45 000 000 XAF** |
| **Formation des utilisateurs** | | | | | | | | | | | | | | **402 000 000 XAF** |
| **Formation des intendants de données** | Formation avancée en transformation des données, IA, assurance qualité des données et gouvernance des données - 12 intendants de données | | | | | | | | | | | | | **30 000 000 XAF** |
| **Formation des utilisateurs niveau central** | Formation à la création, à la transformation et à la visualisation de produits de données - 130 | | | | | | | | | | | | | **372 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | utilisateurs au niveau central | | | | | | | | | | | | | |
| **Équipement informatique** | | | | | | | | | | | | | | **92 000 000 XAF** |
| **Équipement informatique pour les administrateurs système et les gestionnaires de données** | Ordinateurs portables pour 13 membres du personnel | | | | | | | | | | | | | **20 000 000 XAF** |
| **Equipement informatique pour les utilisateurs centraux** | Ordinateurs portables pour 120 membres du personnel | | | | | | | | | | | | | **72 000 000 XAF** |
| **Améliorer l'utilisation des données** | | | | | | | | | | | | | | **240 000 000 XAF** |
| **Développement de cas d'utilisation avancés** | Formations sur l'IA et configuration de rapports spécifiques ; Consultants en science des données | | | | | | | | | | | | | **75 000 000 XAF** |
| **Développement de nouveaux cas d'usage** | Formations sur l'utilisation des données, la visualisation et l'identification | | | | | | | | | | | | | **90 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | des besoins en matière d'intégration des données et de surveillance des maladies dans l'approche « Une seule santé » | | | | | | | | | | | | | |
| **Formation des décideurs de haut niveau** | Formation de 20 directeurs et secrétaires généraux | | | | | | | | | | | | | **30 000 000 XAF** |
| **Réunions trimestrielles sur l'examen des données One Health** | Élaborer un bulletin trimestriel « Une seule santé » en collaboration avec les points focaux de la COHIS | | | | | | | | | | | | | **20 000 000 XAF** |
| **One Health Bulletin** | Élaborer un modèle de bulletin « Une seule santé » | | | | | | | | | | | | | **25 000 000 XAF** |
| **Gouvernance des données et sécurité de l'information** | | | | | | | | | | | | | | **286 000 000 XAF** |
| **Formation annuelle sur la** | Formation des utilisateurs au | | | | | | | | | | | | | **50 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **qualité des données et la sécurité de l'information** | niveau central sur la qualité des données et la sécurité de l'information - 20 utilisateurs | | | | | | | | | | | | | |
| | Formation des utilisateurs au niveau régional sur la qualité des données et la sécurité de l'information - 100 utilisateurs | | | | | | | | | | | | | **200 000 000 XAF** |
| **Audits annuels de sécurité et de gouvernance** | Audit technique et organisationnel des ressources humaines | | | | | | | | | | | | | **36 000 000 XAF** |
| **Gestion des connaissances et échange de bonnes pratiques** | | | | | | | | | | | | | | **106 000 000 XAF** |
| **Voyage d'étude** | Unité de traitement des données, unité de sécurité des données, points focaux COHIS et décideurs | | | | | | | | | | | | | **50 000 000 XAF** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Soutien à d'autres pays et organisations dans le cadre de l'intégration des données One Health** | Missions à court terme en Afrique de l'Ouest et du Centre de gestionnaires de données pour promouvoir et soutenir l'adoption de COHIS et l'intégration des données One Health dans d'autres pays | | | | | | | | | | | | | **36 000 000 XAF** |
| **Documentation et communication** | Vidéos, articles, conférences nationales et internationales | | | | | | | | | | | | | **20 000 000 XAF** |
| **Stratégie et Suivi-évaluation** | | | | | | | | | | | | | | **56 000 000 XAF** |
| **Elaboration de la feuille de route 2027-2028 de la COHIS** | Atelier avec 25 participants techniques | | | | | | | | | | | | | **20 000 000 XAF** |
| **Atelier annuel sur l'suivi-évaluation** | Atelier annuel de suivi-évaluation - 20 personnes | | | | | | | | | | | | | **36 000 000 XAF** |

| | |
|---|---|
| **TOTAL** | **1 567 000 000 XAF** |