République Démocratique du Congo

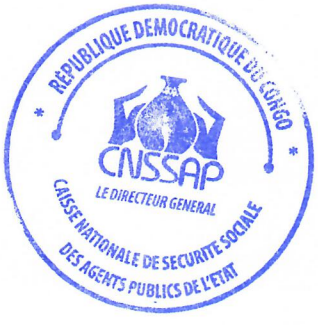
Politique Cadre de la Sécurité du Système d'Information de la CNSSAP

Version PCSSI 2.0

Mars 2024

CNSSAP

HISTORIQUE DES MODIFICATIONS		
Version	**Date**	**Motif des modifications**
Version 1.0	17/06/2021	Création
Version 2.0	05/03/2024	Mise à jour



Sommaire

I. Introduction

I.1. Généralités

L'information est un moyen de production qui, à l'instar d'autres moyens de production importants, représente une valeur considérable qui doit être protégée de manière appropriée.

La sécurité de l'information consiste à protéger les informations traitées par la Caisse Nationale de Sécurité Sociale des Agents Publics de l'État « CNSSAP » d'une multitude de risques, qu'il s'agisse de menaces (actions extérieures ou intérieures malveillantes) ou de vulnérabilités (risques propres aux systèmes et applications), et permet ainsi de garantir la confidentialité, l'intégrité ainsi que la disponibilité des données.

Cette sécurité doit être assurée par la mise en œuvre de mesures adéquates regroupant les structures organisationnelles, les règles, les processus, les procédures mais également le système d'information.

L'ensemble de ces mesures doivent être déterminées et documentées, implémentées, auditées et améliorées aussi souvent que nécessaire, et ce, de manière à atteindre les objectifs spécifiques en matière de sécurité de l'information.

L'analyse des risques doit considérer à la fois la sécurité physique, la sécurité au niveau système, la sécurité au niveau applicatif, la sécurité au niveau réseau et communication, etc.

Le Management (comité décisionnel) fournit les conseils et le soutien nécessaires pour la mise en place de la sécurité de l'information.

La CNSSAP a toujours accordé une importance particulière à la protection des données et informations de son personnel et de ses assurés et elle s'engage strictement à respecter les dispositions législatives et réglementaires qui encadrent et qui régissent l'utilisation des données et des informations, ainsi que les principes de sécurité de l'information :

- **La confidentialité** : le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître ;
- **L'intégrité :** La protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci ;
- **La disponibilité :** L'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

Par conséquent, la CNSSAP élabore cette politique de sécurité de l'information qui définit les objectifs et les mécanismes de l'organisation de la sécurité de l'information à déployer et à mettre en place.

I.2. Objectifs

Les objectifs de la politique de sécurité de l'information sont :

1. Protéger la réputation, l'intégrité, l'éthique, et l'image publique de la CNSSAP.
2. Maintenir la confiance des clients, fournisseurs ainsi que des partenaires de la CNSSAP.
3. Protéger le caractère confidentiel de l'information sensible.
4. Protéger les données opérationnelles sensibles des divulgations inappropriées.

5. Prévenir les tiers contre les actes illégaux ou malveillants à l'encontre des systèmes d'information de la CNSSAP.
6. Assurer la non-répudiation : Permet de garantir qu'une transaction ne peut être niée.
7. Vérifier l'authentification : Consiste à s'assurer de l'identité d'un utilisateur et garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. L'authentification est nécessaire pour la non-répudiation.
8. Assurer la traçabilité : Consiste à conserver une trace probante : originale, horodatée, explicite et intègre, d'un évènement technique (ex : Traces techniques de sécurité ou logs) ou d'un acte métier (ex : piste d'audit). Pour être probante, une trace doit pouvoir être rattachée à un acteur et à une référence au temps fiables.
9. Optimiser l'utilisation des ressources du SI-CNSSAP en s'assurant de leur bonne utilisation.
10. Prévenir contre les fraudes.
11. Prévenir contre les incidents importants qui peuvent occasionner des ruptures de l'activité.
12. Se conformer aux exigences réglementaires et légales.
13. Supporter les objectifs métiers de la CNSSAP.
14. Réduire le risque de perte de confidentialité, d'intégrité et de disponibilité de l'information, en définissant des principes de l'usage et du traitement de l'information.
15. Assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère personnel relatifs au personnel de la CNSSAP et à tous ses partenaires.
16. Etablir un Plan de Continuité d'Activités pour la CNSSAP.

I.3. Champs d'Application

La Politique de sécurité de l'information s'applique à :

1. L'information dans toutes ses formes, résidant sur des serveurs, des ordinateurs, des équipements réseaux ou autres, les bases de données, les documents personnels, dossiers et documents de travail.
2. Toutes les Applications, Systèmes d'Exploitation, Progiciels et Logiciels.
3. Tous les Matériels, Firewalls, Serveurs, postes de travail, Laptops, composants du réseau, équipements de communication et périphériques possédés.
4. Tous les sites de la CNSSAP qui hébergent les informations et les systèmes supports.
5. L'ensemble du personnel de la CNSSAP tant interne qu'externe, permanents, contractuels, temporaires, consultants, fournisseurs, prestataires tiers, etc.
6. Tous les systèmes d'informations développés, opérationnels et à développer.
7. La protection de l'information s'appuie sur l'engagement continu de l'ensemble du personnel de la CNSSAP. Chacun a l'obligation de protéger l'information et le matériel mis à sa disposition. Chaque intervenant a des responsabilités spécifiques en matière de sécurité et est redevable de ses actions. Ainsi, les rôles et responsabilités de tous les intervenants sont clairement définis dans cette Politique.

I.4. Références légales et normatives

Les principes directeurs qui sous-tendent ces Politiques sont tirés essentiellement des bonnes pratiques des normes internationales suivantes :

1- Norme internationale ISO 27001 :2022 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences.
2- Norme internationale ISO 27002 :2022 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information.
3- Norme internationale ISO 27005 :2022 : Techniques de sécurité – Gestion du risque en sécurité de l'information.
4- Norme internationale ISO/CEI 27000 : 2018, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire.
5- Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique en RDC.

I.5. Elaboration

1- Les politiques de sécurité de l'information sont élaborées par le Chef de Département Sécurité des Systèmes d'Information (CDSSI) sous la supervision du Directeur des Systèmes d'Information (DSI) et validées par le Directeur général.
2- Le Manuel des politiques de sécurité de l'information est mis à jour chaque trois ans, ou lors de changements significatifs qui pourraient l'affecter.
3- Toutes les versions sont conservées sous forme électronique. La version française originale sous forme « papier » constitue la version de référence.

II. Politiques de la sécurité de l'information

II.1. Responsabilités

A. Le Directeur général (DG)

1- Approuve une politique de sécurité simple, précise, compréhensible et applicable ;
2- Accrédite le respect de toutes les contraintes légales et réglementaires et veille au respect de cette Politique par tous les intervenants internes et externes au niveau de la CNSSAP ;
3- Apporte les ressources nécessaires pour la réussite de la politique de sécurité au sein de la CNSSAP ;
4- Assure le suivi de la réalisation des objectifs de la sécurité de l'information.

B. Le Directeur des systèmes d'information (DSI)

1- Veille et s'assure du respect des principes suivants :
   - ✓ **L'intégrité** : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.
   - ✓ **La confidentialité** : Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
   - ✓ **La disponibilité** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues ; garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
   - ✓ **La non-répudiation et l'imputation** : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
   - ✓ **L'authentification :** L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
2- Discute et approuve les objectifs stratégiques de Sécurité du système d'information de la CNSSAP ;
3- Oriente les mesures à prendre en matière de sécurité du système d'information, s'assure de leur formalisation par des Politiques de sécurité de l'information, valide ces politiques, approuve la périodicité de leur mise à jour et en assure le suivi de leur mise en place ;
4- S'assure que les activités de la CNSSAP soient menées en conformité avec :
   - Les politiques internes de sécurité de l'information ;
   - Les réglementations externes de sécurité de l'information ;
5- Porte une appréciation sur les actions à prendre et qui sont en relation avec la formation, la qualification et le recyclage des ressources humaines chargées de la Sécurité du Système d'Information ;
6- Assure le suivi de la réalisation des projets et/ou des actions en relation avec la sécurité du système d'information ;
7- Assure le suivi des incidents du système d'information, définit des recommandations pour leur résolution et s'assure de leur réalisation dans les délais convenus par un suivi permanent des avancements des travaux ;

8- Assure un suivi régulier de la situation sécuritaire du système d'information de la CNSSAP par des indicateurs et des tableaux de bord de sécurité, ainsi que par le suivi de la réalisation des plans d'actions arrêtés dans :
   - Les rapports d'audit informatique ;
   - Le Plan de Continuité des Activités (PCA).

C. Le Chef de Département Sécurité des Systèmes d'Information (CDSSI)

Le Chef de Département Sécurité des Systèmes d'Information (CDSSI), doit :

1. Coordonner la mise en œuvre de toutes les tâches de la sécurité de l'information ;
2. Piloter et implémenter la mise en place de la politique de sécurité de l'information, effectuer le contrôle, le suivi et les reporting sécurité.
3. Elaborer en collaboration avec l'Administration, le programme de Sensibilisation à la Sécurité de l'Information et s'assurer de sa mise en place.
4. Mettre en place une stratégie et une approche pour détecter les risques en matière de la Sécurité de l'Information.
5. Revoir périodiquement la Politique de la Sécurité de l'Information et proposer des recommandations d'amélioration au Directeur général pour avis et appréciation.
6. Elaborer et faire valider selon le processus décrit ci-dessus, les documents liés aux processus de sécurité, directives, standards, et stratégies spécifiques en cas de besoin.
7. Examiner les incidents de la sécurité de l'information en collaboration avec les différents utilisateurs impliqués, et soumettre des rapports au Directeur général pour avis, appréciation et mise en place des ressources si nécessaire.
8. Conseiller sur les aspects de la sécurité de l'information, le plan de continuité d'activités et le plan de secours.
9. S'assurer que les Politiques de Sécurité sont appliquées par des tests périodiques de conformité et en cas de violation, faire un rapport d'alerte au Directeur général pour prise de décision.
10. Effectuer les estimations périodiques des risques liés aux Technologies de l'information et de la communication.
11. Travailler en étroite collaboration avec les Correspondants de la Sécurité pour assurer et satisfaire les exigences des Politiques de Sécurité de l'Information de la CNSSAP.
12. Assister aux différents forums spécialisés dans la sécurité de l'information.

D. Le Chef de Département Systèmes, Réseaux et Sécurité (CDSRS) / Chef de Département Conception et Développement (CDCD) / Chef de Département Exploitation du Système d'Information (CDESI)

Les Chefs de Département doivent :

1- Assurer la sauvegarde et la restauration des données;
2- Gérer et administrer les informations des applications ;

3- Etablir les contrôles de sécurité des systèmes d'exploitation, Applications et Bases de données ;
4- Assurer une réaction rapide aux incidents de sécurité ;
5- Participer à la mise en œuvre du plan de continuité des activités (PCA).

E. Le Directeur Juridique et du Contentieux (DJC)

1- Le Directeur Juridique et du Contentieux (DJC) conseille et assiste le Management quand une atteinte à l'intégrité physique ou logique du système informatique est identifiée ;
2- Il s'assure de la légalité des actions prises ainsi que leur conformité à la réglementation applicable (Articles 337, 339 et 340 de l'ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique en RDC).

F. Le Directeur du Contrôle et Gestion des Risques (DCGR)

1- Le Directeur de Contrôle et Gestion des Risques (DCGR) s'assure que les politiques de sécurité de l'information sont conformes aux lois, aux réglementations et aux normes en vigueur dans la sécurité sociale ;
2- Il examine les politiques de sécurité de l'information existantes pour évaluer leur pertinence, leur efficacité et leur conformité aux objectifs de l'établissement ;
3- Il joue un rôle actif dans le processus d'élaboration des politiques de sécurité de l'information en apportant son expertise et ses recommandations basées sur les risques identifiés.
4- En collaboration avec les parties prenantes, l'audit interne peut contribuer à la création de directives et de procédures détaillées pour mettre en œuvre les politiques de sécurité ;
5- Il surveille régulièrement la conformité aux politiques de sécurité de l'information en effectuant des audits et des vérifications périodiques ;
6- Il participe à l'élaboration de plans de gestion des incidents de sécurité et à la mise en œuvre de procédures pour répondre efficacement aux incidents ;
7- Il prépare des rapports périodiques sur l'état de la sécurité de l'information, les résultats des audits, les risques identifiés et les recommandations.

G. Les différents intervenants au niveau de la CNSSAP

1- Le Chef de Département Sécurité des Systèmes d'Information (CDSSI) est responsable de la mise à jour des Politiques de Sécurité de l'information ainsi que des directives associées dans le respect de la chaîne de validation.
2- Le Directeur des Ressources Humaines (DRH) en collaboration avec le **CDSSI**, est responsable de la formation, le recyclage et la qualification des employés chargés de la sécurité de l'information ainsi que de la sensibilisation de tout le personnel de la CNSSAP aux politiques de sécurité de l'Information par des campagnes périodiques et bien orientées.
3- Tous les utilisateurs internes et externes (employés, conseillers, experts, auditeurs, temporaires, etc.) ayant des informations (électroniques, papiers) au niveau de la CNSSAP sont responsables

de la protection de l'information dont ils sont propriétaires et/ou sous leur contrôle, conformément aux politiques de sécurité de l'information.

L'utilisateur est un acteur important de la sécurité des SI, son implication se fait à trois niveaux :

- ✓ **Respect des règles :** Chaque utilisateur doit respecter les règles de sécurité édictées, respecter les dispositifs de sécurité et observer les mesures édictées.
- ✓ **Prudence** : Chaque utilisateur doit agir avec discernement et appliquer un principe de précaution vis à vis de tout comportement potentiellement à risque pour la sécurité du système d'information.
- ✓ **Vigilance :** Tout utilisateur doit informer sa hiérarchie et son correspondant sécurité de tout incident ou anomalie constatée (devoir d'alerte).

4- Toute personne ayant accès aux actifs informationnels assume des responsabilités spécifiques en matière de sécurité. Elle applique et respecte la politique de sécurité et ses normes et procédures ainsi que les lois et règlements spécifiques à son domaine d'activité. Elle avise son supérieur immédiat de toute situation susceptible de compromettre la sécurité des actifs informationnels ;

5- Tous les intervenants au niveau de la CNSSAP doivent participer activement à la protection de l'information dans leurs activités quotidiennes. Ils doivent en outre :

- ✓ Utiliser les ressources informationnelles en se limitant aux fins pour lesquelles elles sont destinées et dans le périmètre des accès qui leurs sont autorisés ;
- ✓ Respecter le caractère confidentiel des renseignements auxquels ils ont accès ;
- ✓ Assurer la sécurité des actifs informationnels de la CNSSAP au meilleur de leurs connaissances et en fonction de leurs rôles et responsabilités ;
- ✓ Aviser l'équipe informatique de toute situation susceptible de compromettre la sécurité du personnel et/ou des actifs informationnels ;
- ✓ Appliquer et respecter l'ensemble des points de la politique de sécurité de l'information ainsi que toute autre politique, directives, normes ou procédures édictées par la CNSSAP.

6- Aucune exception à ces politiques n'est autorisée sans une approbation écrite du Directeur général à la suite d'une proposition formulée par le Chef de Département Sécurité des Systèmes d'Information (CDSSI) et dûment signée.

II.2. Conformité

Tout le Personnel de la CNSSAP qui utilise les actifs informationnels (électroniques/papiers) doit se conformer aux dispositions de la Politique de Sécurité de l'Information ainsi qu'à toutes les directives, procédures et standards qui s'y rattachent.

Tout employé qui ne respecte pas la politique de sécurité de l'information est considéré comme étant en violation du Code de conduite des employés de la CNSSAP et doit être sujet à des mesures disciplinaires ou à des sanctions appropriées.

II.3. Contact

1- Toutes les questions concernant la politique de sécurité doivent être adressées au Chef de Département Sécurité des Systèmes d'Information (CDSSI).
2- Tous les incidents liés à la sécurité ou leurs violations doivent être rapportés immédiatement et sans délai au CDSSI par e-mail ou par tout autre moyen laissant une trace écrite.
3- Le CDSSI doit coordonner les activités avec les différentes autorités compétentes aussi bien internes qu'externes en matière de sécurité de l'information.

II.4. Révision de la politique de sécurité de l'information

1- La politique de sécurité de l'information doit être révisée chaque trois ans et modifiée lorsque des changements sont nécessaires afin de tenir compte de l'évolution de la menace, des risques et des besoins de la CNSSAP.
2- Toute modification apportée à la présente politique doit être validée par le Directeur des Systèmes d'Information (DSI) et approuvée par le Directeur général ;
3- Les révisions et les mises à jour ne doivent pas déroger aux mesures de la norme ISO : 27002 qui définit la sécurité de l'information comme : la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».

II.5. Accès à distance aux systèmes d'informations de la CNSSAP

1- Les accès à distance aux réseaux et aux ressources de la CNSSAP sont accordés uniquement aux utilisateurs autorisés et authentifiés et disposant de privilèges restreints.
2- L'usage des « Mobile Phone » professionnel et personnel doit être conforme à la Politique BYOD.
3- L'employé autorisé à effectuer des voyages d'affaires pour le compte de la CNSSAP, doit veiller au respect de la sécurité de l'information et doit sécuriser les appareils (mobile phone et PC) en sa possession contre les risques de perte et de vol.
4- L'usage d'un ordinateur portable en dehors des locaux de la CNSSAP est accordé selon la procédure en vigueur, et son usage doit être purement professionnel.
5- Chaque utilisateur doit se limiter à un usage strictement professionnel de l'équipement mis à sa disposition (ordinateur portable, mobile phone, etc.) par la CNSSAP, ce qui exclut l'utilisation à des fins personnelles.
6- L'utilisateur est responsable de la sécurité et la sauvegarde des données sur les appareils mobiles mis à sa disposition.

NB : Les utilisateurs autorisés à travailler à distance doivent veiller sur la sécurité des informations consultées, traitées ou stockées.

II.6. Attribution des droits d'accès aux systèmes d'informations

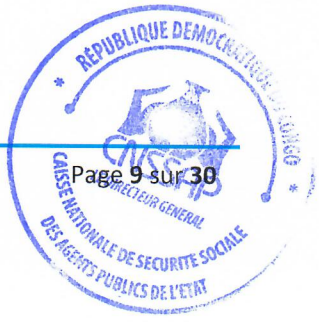
- **Les services/directions concernés de la CNSSAP, doivent :**

1- Assurer la sécurité des actifs informationnels par un processus formel de gestion et de contrôle des codes et profils d'accès accordés à ses utilisateurs ;
2- Définir les mesures de gestion et d'utilisation sécuritaire des mots de passe. Chaque utilisateur doit avoir une identification unique (Login/ Mot de passe) sur le réseau et les systèmes d'information, et tout partage des Login/ Mot de passe doit être strictement interdit ;

3- Assurer la présence des contrôles adéquats (journaliers) pour détecter, vérifier et valider les accès aux systèmes et le respect des mesures et procédures de sécurité de la CNSSAP ;
4- Assurer une révision et un réexamen annuel des droits d'accès des utilisateurs du SI-CNSSAP ;
5- Assurer une suppression ou une désactivation des droits d'accès des utilisateurs au SI à la fin de leur période d'emploi, ou une modification en cas de changement de contrat ou de mutation (la notification de départ du personnel ou de mutation doit émaner du DRH au DSI et à l'équipe informatique).

- **Les mesures techniques à prendre par l'équipe de la Direction des Systèmes d'Information pour assurer les règles de gestion sont les suivantes :**

1. Seules les personnes autorisées ont un droit d'accéder aux données sensibles et confidentielles de la CNSSAP ;
2. L'information liée aux données des employés doit être protégée et ne peut être consultée et mise à jour que par le personnel autorisé ;
3. Les ressources très sensibles doivent être isolées ;
4. L'accès au système doit être soumis à une procédure sécurisée d'ouverture de session. Il est géré et surveillé par la Direction des Systèmes d'Information pour identifier les mauvaises utilisations du système d'information ;
5. Tous les systèmes doivent produire des journaux, qui doivent être contrôlés par les unités concernées ;
6. Les informations contenues dans les journaux doivent être pertinentes pour supporter des éventuelles enquêtes ;
7. Les alertes pour usage non autorisé des systèmes internes critiques doivent être journalisés et remontés au CDSSI ;
8. La sélection des mots de passe, leur usage et leur gestion est un moyen important pour le contrôle d'accès aux systèmes ;
9. Le recours aux programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être très limité et bien contrôlé ;
10. Des procédures de contrôle des bibliothèques de code source doivent être établies et respectées ;
11. L'intégrité du code source du logiciel opérationnel de la CNSSAP doit être protégée en utilisant notamment des techniques de contrôle d'accès ;
12. L'accès en mode commande (ou graphique) aux systèmes doit être restreint au personnel administrateur des systèmes.
13. Les procédures de contrôle d'accès distants doivent fournir des protections adéquates à travers l'identification robuste, l'authentification et les techniques de cryptage ;
14. Toutes les actions, y compris l'administration du système, doivent être exécutées avec les autorisations minimums exigées pour conduire l'activité ;
15. L'abus des niveaux de l'autorité, et les accès non autorisés sont considérés comme des fautes professionnelles.



- **Partage d'accès à l'information :**

1- Toutes les données partagées sur le serveur de fichiers sont classées « confidentiel » et ne sont par conséquent, disponibles qu'aux personnes autorisées ;
2- Les données de l'employé ne peuvent être communiquées et mises à jour que par les personnes autorisées.

- **Contrôle d'accès à l'Internet, Intranet et Extranet :**

1- Le personnel responsable de l'installation et de la configuration des accès à l'Intranet, doit s'assurer que toutes les restrictions d'accès qui concernent les données sur le SI sont bien mises en place au niveau des accès à l'Intranet de la CNSSAP ;
2- Le personnel responsable de l'installation et de la configuration des accès à l'Extranet, doit s'assurer que toutes les restrictions d'accès qui concernent les données sur le SI, sont bien mises en place au niveau des accès à l'Extranet de la CNSSAP ;
3- Le personnel responsable de l'installation de l'Internet, doit s'assurer que le réseau de la CNSSAP est protégé contre les accès et intrusions malicieuses, en déployant la configuration des Firewalls nécessaires ;
4- Le Chef de Département Sécurité des Systèmes d'Information (CDSSI) est chargé du contrôle et de la surveillance des accès des utilisateurs à l'Internet. Le CDSSI doit sensibiliser les utilisateurs aux risques et menaces de l'Internet, et ce, par des sessions de sensibilisation régulières.

II.7. Traitement des exceptions au manuel de la politique

Le manuel de la politique cadre de sécurité de l'information a été rédigé afin d'atteindre au moins les protections stipulées dans les lois et réglementations en RDC, notamment l'ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique. Toute politique de sécurité de l'information de la CNSSAP jugée comme contradictoire aux lois et réglementations en vigueur, devra être immédiatement rapportée au Chef de Département Sécurité des Systèmes d'Information (CDSSI).

Les exceptions au manuel de la politique cadre de sécurité de l'information ne sont permissibles que si une analyse de risques concernant la non-conformité a été réalisée et l'exception approuvée par l'équipe informatique.

III. Politiques de la sécurité des ressources humaines

1- Le Directeur des Ressources Humaines (DRH) doit :
- ✓ Informer toute nouvelle recrue (stagiaire, temporaire, contractuelle) de ses obligations découlant de la présente politique ;
- ✓ Sensibiliser toute nouvelle recrue aux enjeux liés à la sécurité des actifs informationnels ;
- ✓ S'assurer de l'existence des clauses relatives au secret professionnel et à la confidentialité des données conformément aux dispositions internes, mais aussi à l'ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique en RDC ;

- ✓ Superviser la mise en place d'un programme continu de sensibilisation et de formation à la sécurité des actifs informationnels pour tout le personnel de la CNSSAP ;
- ✓ S'assurer que tout le personnel de la CNSSAP est systématiquement informé des nouvelles menaces et des nouvelles techniques sur la sécurité de l'information ;
- ✓ Aviser sans délai et par écrit les unités concernées pour faire le nécessaire quant à la politique de sécurité de l'information en cas de fin de contrat sous n'importe quelle forme : départ à la retraite, décès, fin de stage, fin de contrat, etc.

2- La nouvelle recrue doit prendre connaissance de la politique de sécurité de l'information, et doit s'engager à :

- ✓ Respecter la politique de sécurité de l'information ainsi que les normes, directives et procédures en vigueur qui en découlent.
- ✓ Aviser le supérieur hiérarchique dès qu'il constate un manquement à cette politique.

IV. Politiques de la manipulation des supports des actifs informationnels

1- Seul le personnel qui a la responsabilité des installations et des mises à jour est autorisé à utiliser les supports amovibles. Toute autre personne doit avoir une autorisation préalable et spécifique de la hiérarchie.
2- Tous les périphériques d'origine de l'ordinateur (CD, disquette, Bandes, etc.) et les médias qui contiennent des informations sensibles doivent être bien référenciés, gardés dans un emplacement sécurisé.
3- Tous les médias en transit sont sous la responsabilité de leur Superviseur (porteur).
4- Tous les médias doivent être stockés et utilisés, conformément aux exigences du fabriquant.
5- Les supports contenant des informations sensibles doivent être stockés et mis au rebut d'une façon sûre et sécurisée, par exemple par incinération ou déchiquetage, ou par effacement des données pour qu'ils puissent resservir dans d'autres applications ;
6- La mise au rebut des supports contenant des informations doit être appliquée selon une procédure et cette action doit être journalisée afin d'assurer une traçabilité comme une piste d'Audit ;
7- Les supports contenant l'information doivent être protégés contre les accès non autorisés, les erreurs d'utilisations et l'altération lors de leurs éventuels transports.

V. Politiques de cryptographie

La cryptographie est une technique permettant d'assurer la sécurité et la confidentialité des données dans les systèmes d'Informations et de Communications. Elle permet de protéger et d'authentifier l'échange d'informations pour réaliser les propriétés de sécurité :

- Confidentialité ;
- Intégrité ;
- Authentification.

On utilise des crypto systèmes basés sur des fonctions de chiffrement et/ou de déchiffrement et des clés.

1. La politique de cryptographie de la CNSSAP doit :
   - Tenir compte de la réglementation et des restrictions nationales pouvant s'appliquer aux techniques cryptographiques ;
   - Comporter les exigences de gestion des clés cryptographiques couvrant l'ensemble de leur cycle de vie : génération, stockage, archivage, extraction, attribution, retrait et destruction des clés ;
2. Les algorithmes de chiffrement, ainsi que la longueur des clés, doivent être conformes aux bonnes pratiques. Une gestion appropriée des clés exige des processus sécurisés de génération, de stockage, d'archivage, d'extraction, d'attribution, de retrait et de destruction des clés cryptographiques ;
3. Les clés cryptographiques doivent être protégées contre tout risque de modification ou de perte. En outre, il est nécessaire de protéger les clés secrètes et privées contre toute utilisation, ainsi que contre toute divulgation non autorisée ;
4. Une protection physique du matériel utilisé pour générer, stocker et archiver les clés, doit être assurée ;
5. Afin de réduire la probabilité d'utilisation abusive des clefs, il convient de fixer des dates d'activation et de désactivation, de sorte que les clés ne puissent être utilisées que pendant la période de temps définie dans la politique de gestion des clés correspondante ;
6. Des certificats de clés publiques, délivrés par une autorité de certification peuvent être utilisés par la CNSSAP. Dans ce cas, des accords de service et contrats doivent être conclus avec l'autorité de certification. Les questions de responsabilité juridique, de fiabilité des services et de réactivité dans la fourniture de ces services doivent y être indiquées.
7. La CNSSAP doit veiller au chiffrement des données sensibles, en particulier sur les postes nomades et sur les supports potentiellement perdables.
8. Plusieurs produits de chiffrement de disques ou de partitions (ou supports chiffrant) ont été qualifiés par l'ANSI. Il convient de les utiliser en priorité. La qualification par les organismes spécialisés garantit la robustesse des mécanismes cryptographiques mis en œuvre.
9. Le chiffrement peut être réalisé sur l'ensemble du système (on parle de chiffrement intégral), sur un sous-ensemble du système (chiffrement de partitions) ou sur les fichiers les plus sensibles. Les mécanismes de chiffrement intégral de disque sont les plus efficaces du point de vue de la sécurité et ne nécessitent pas pour l'utilisateur d'identifier les fichiers à chiffrer. Dans les cas où la mise en œuvre de ce type de système de chiffrement s'avère trop complexe, il est impératif de mettre à disposition des utilisateurs un système de chiffrement de partitions.
10. Tout support amovible peut facilement être égaré ou volé. Il convient donc de chiffrer également les disques USB externes. Le chiffrement des disques internes et externes s'effectue en suivant les recommandations de l'équipe informatique.
11. Les clés USB ne doivent être utilisées que pour transférer les données et non pas comme un moyen de stockage (risque de perte de données important). Si la clé USB est utilisée pour transporter des données sensibles, il est recommandé d'utiliser les clés USB auto-

chiffrantes préconisées par l'équipe informatique pour éviter le vol de données en cas de perte de la clé.

VI. Politiques de la sécurité physique et de l'environnement

1- Le matériel et équipement doit être protégé, des pannes de courant et autres anomalies. Un système de protection contre les surtensions (onduleurs) doit être utilisé, conformément aux spécifications des fournisseurs du matériel et selon les procédures en vigueur.
2- Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de la CNSSAP en tenant compte des risques associés au travail hors site.
3- L'équipe informatique doit s'assurer que tout le matériel contenant des supports de stockage ne contient pas de stockage de données sensibles et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ;
4- Il faut détruire physiquement les appareils contenant des informations sensibles ou, supprimer ou écraser les informations au moyen de techniques empêchant de retrouver l'information d'origine, plutôt que par la fonction standard de suppression ou de formatage ;
5- Les équipements et dispositifs de stockage qui contiennent des informations sensibles et qui sont jugés non exploitables doivent être physiquement détruits ;
6- Les ordinateurs endommagés contenant des données sensibles peuvent nécessiter une appréciation du risque visant à déterminer s'il convient de les détruire physiquement plutôt que de les envoyer en réparation ou de les mettre au rebut ;
7- Toute nouvelle installation de matériel ou application critique doit être formellement planifiée et notifiée à toutes les parties concernées avant la date de l'installation proposée. Les exigences de la sécurité doivent être communiquées à toutes les parties concernées, avant l'installation ;
8- Tout le matériel fourni doit être complètement testé et formellement accepté par l'équipe informatique avant d'être transféré en production ;
9- Le matériel sensible ou précieux (bandes de sauvegarde, …) doit être stocké avec les précautions nécessaires.

VII. Politiques de la sécurité de l'exploitation des moyens de traitement de l'information

1. Les données/informations sensibles ou confidentielles, ne peuvent pas être transférées via les réseaux, ou copiées sur un autre support, sauf si le caractère confidentiel et l'intégrité des données sont raisonnablement assurés.
2. Les informations sensibles ou confidentielles ne doivent pas être communiquées via les téléphones fixes, sauf si les méthodes et techniques de sécurité de transmission sont assurées ;
3. Les informations classées comme « Confidentielles » ou « Secrètes » ne doivent jamais être envoyées vers une imprimante réseau sauf si une personne autorisée est disponible pour

récupérer les documents imprimés et assurer leur caractère confidentiel pendant et après l'impression ;

4. La sauvegarde et la restauration de données sont d'une priorité maximale pour la CNSSAP. La Direction des Systèmes d'Information doit s'assurer que les procédures de sauvegarde et de restauration sont mises en place, documentées et que la fréquence des opérations est conforme aux besoins ;
5. Le stockage quotidien des données doit assurer leur disponibilité aux utilisateurs autorisés. Les archives doivent être accessibles en cas de besoin afin d'assurer la continuité d'activité de la CNSSAP ;
6. L'archivage des documents doit être conforme aux procédures en vigueur et à la réglementation ;
7. Tous les utilisateurs du système d'information, qui sont amenés à créer ou à modifier des fichiers de données, doivent enregistrer régulièrement leur travail sur le système ;
8. Les médias des stockages utilisés pour l'archivage de l'information doivent être appropriés pour la longévité ;
9. Les formats dans lesquels les données sont stockées doivent être bien étudiés (supports de stockage et moyens de traitement), en particulier lorsque les formats des données sont propriétaires ;
10. Des essais sur les supports de sauvegarde et de restauration doivent être régulièrement effectués pour s'assurer de leur fiabilité en cas d'utilisation en urgence ;
11. Les supports de sauvegarde doivent être placés dans un endroit suffisamment éloigné pour échapper aux dommages d'un sinistre sur le site principal ;
12. Des procédures doivent être établies pour la gestion et le contrôle des modifications des systèmes en production. Tout changement aux programmes doit être préalablement testé dans un environnement de test approprié avant d'être autorisé à être mis en œuvre sur les systèmes en production ;
13. Les opérations effectuées sur les systèmes doivent être formellement documentées, planifiées et autorisées ;
14. Les mises à jour des applications/logiciels et systèmes doivent être testées par un personnel qualifié avant leur mise en œuvre dans l'environnement de production ;
15. Les correctifs et patchs de sécurité ne peuvent être appliqués qu'après vérification de leur nécessité et autorisation du Directeur de Système d'Information (DSI). Ils doivent être d'une source confirmée et être testés avant leur mise en œuvre dans l'environnement de production ;
16. La décision de mettre à jour des applications/logiciels et systèmes ne peut être prise qu'après considération des risques associés à la mise à jour et à l'étude des bénéfices de la mise à jour et de sa nécessité ;
17. La séparation des équipements de développement, de test et de production doit être assurée afin de réduire les risques d'accès ou de changements non autorisés dans les systèmes en production ;
18. Les nouvelles applications, acquises ou développées en interne par l'équipe informatique doivent disposer d'un module de journalisation ;

19. Les Systèmes d'exploitation doivent être régulièrement surveillés. Leurs horloges doivent être synchronisées. Un réexamen périodique des résultats des activités de surveillance doit être établi par les acteurs concernés ;
20. Les messages d'erreurs ou défaillances des logiciels et applications doivent être enregistrés et reportés à la Direction des Systèmes d'Information en cas de besoin ;
21. Le matériel, les systèmes, logiciels, applications et réseaux doivent être correctement configurés et protégés contre les attaques physiques, les intrusions et les accès non autorisés ;
22. Les lignes de transport externes de données sensibles devront permettre l'utilisation de canaux cryptés (La technologie VPN) ;
23. Afin de réduire la fréquence des attaques/intrusions internes ou externe, des contrôles et techniques de sécurité doivent être mis en œuvre : Firewall, etc.
24. Le site Web de la CNSSAP, doit être minutieusement configuré par un spécialiste pour assurer une prévention optimale contre les attaques et les intrusions ;
25. Les appels téléphoniques peuvent être interceptés. De ce fait, une extrême prudence doit être prise lors des discussions traitant des informations classées « secret » ;
26. Les systèmes d'informations doivent être administrés en utilisant des procédures documentées afin d'assurer l'efficacité et la sécurité nécessaire ;
27. Pour tous les systèmes d'informations, la documentation doit être régulièrement tenue à jour et disponible pour tout le personnel et les utilisateurs concernés ;
28. Le plan de secours informatique doit être maintenu et périodiquement testé pour s'assurer de son adéquation ;
29. Sans aucune exception, les logiciels antivirus doivent être déployés sur tous les ordinateurs, serveurs, et ce, avec une mise à jour régulière ;
30. Un logiciel de détection d'intrusion (HIDS/IDS) doit être déployé sur les serveurs sensibles et les PCs du personnel stratégique ;
31. Les tests de pénétration doivent être réalisés par des Experts indépendants contractés pour une mission ponctuelle, ayant pour objectif la détection des vulnérabilités dans les systèmes et la vérification de l'efficacité des contrôles existants ;
32. Des précautions doivent être prises lors des tests de pénétration afin de ne pas causer des dénis de service des systèmes en production.

VIII. Politiques de la sécurité de la communication au niveau des réseaux et des moyens de traitement de l'information

1. Le personnel responsable de l'installation et de la configuration des accès à l'Intranet doit s'assurer que toutes les restrictions d'accès qui concernent les données sur les systèmes sont aussi appliquées pour accéder à l'Intranet de la CNSSAP ;
2. Le personnel responsable de l'installation de l'Internet doit s'assurer que le réseau de la CNSSAP est protégé contre les accès et intrusions malicieuses, en déployant la configuration des Firewalls nécessaires.
3. Le site web de la CNSSAP ne doit être développé et maintenu que par des personnes autorisées ;

4. La Direction de Système d'Information est responsable du contrôle et de la surveillance des accès utilisateurs à l'Internet, les utilisateurs doivent être bien sensibilisés aux risques et menaces de l'Internet ;
5. Les réseaux hébergeant des actifs sensibles et les réseaux d'interconnexion permettant d'accéder à ces réseaux doivent isoler les flux utilisateurs des flux d'administration, de supervision, d'alerte et de techniques des équipements ;
6. Tous les éléments composant une chaîne de liaison permettant l'accès à des actifs sensibles en disponibilité doivent être redondés ;
7. L'isolation d'un établissement vis-à-vis des zones externes et publiques, doit être réalisée au moyen d'un pare-feu physique dédié ;
8. L'isolation d'un réseau d'administration et l'isolation vis-à-vis d'un réseau public, doivent être réalisées sur des pare-feu physiquement distincts ;
9. Les règles de filtrage doivent être revues au moins une fois par an de manière à :
    - Identifier les règles obsolètes ;
    - Vérifier le respect de la règle d'interdiction par défaut ;
    - Vérifier l'existence d'une demande validée en regard de chaque règle.
10. Les services fonctionnant sur les équipements d'infrastructure réseau doivent être désactivés ou supprimés lorsqu'ils ne sont pas requis ;
11. Les bannières d'accueil des équipements ou systèmes accessibles depuis un réseau public ne doivent pas contenir d'informations techniques (nom et version du composant, etc.) susceptibles d'être exploitées à des fins malveillantes ;
12. La cartographie du réseau doit :
    - Couvrir tout le périmètre de l'établissement ;
    - Faire figurer le plan d'adressage ;
    - Être maintenue à jour ;
    - Être disponible à tout instant ;
    - Identifier les interconnexions ;
    - Identifier chaque équipement réseau.
13. La cartographie du réseau doit être considérée comme une information sensible ;
14. Les adresses internes à la CNSSAP doivent être « translatées » (NAT) pour accéder aux réseaux externes à la CNSSAP ;
15. Tous les équipements réseaux hébergeant des actifs sensibles doivent être mis à jour dans les 45 jours qui suivent la diffusion des correctifs de sécurité concernant des failles critiques/jugées critiques par l'éditeur ou la Direction de Système d'Information.

IX. Politiques de sécurité des transferts de l'information via Internet et messagerie électronique

1- Les serveurs de messagerie doivent être protégés contre les attaques de type relais de mail ;
2- Les serveurs de messagerie doivent être protégés par des solutions logicielles antivirus et anti-spam ;
3- Tout utilisateur de système de messagerie doit s'assurer que l'information communiquée par email est correctement adressée, et envoyée uniquement aux personnes appropriées ;

4- L'interconnexion à des réseaux externes ne peut avoir lieu qu'à travers des passerelles Internet approuvées ;
5- L'accès d'une partie tierce à l'information de la CNSSAP n'est autorisé qu'en cas de nécessité pour les exigences de la mission qui lui est confiée ;
6- Tous les fournisseurs, prestataires de services, consultants doivent obligatoirement veiller au respect de la Politique de Sécurité de l'Information de la CNSSAP ;
7- L'accès aux ressources sur le réseau doit être strictement contrôlé pour prévenir l'accès non autorisé.

X. Politiques d'acquisition, de développement et de maintenance des systèmes d'information

1- Lors de l'acquisition, du développement et de la maintenance du Système d'Information (SI), il faut mettre en place des règles de gestion pour sécuriser le SI, ces règles doivent être clairement définies et indiquées comme clauses contractuelles ;
2- Les applications critiques métier doivent être vérifiées et testées lorsque des changements sont apportés aux plateformes d'exploitation afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité ;
3- Le développement de logiciel est une activité très technique et doit être entreprise et contrôlée par un personnel autorisé et qualifié ;
4- Un logiciel développé par la CNSSAP doit suivre un processus formalisé de développement;
5- Un logiciel développé doit être conforme aux exigences et besoins des utilisateurs et doit offrir un support approprié ;
6- Toute activité de développement du système externalisée doit être supervisée et contrôlée ;
7- Tous les systèmes doivent être testés avant leur mise en exploitation ;
8- Tous les logiciels doivent être conformes aux préférences existantes en matière de système d'exploitation et de plateforme.

XI. Politiques de sécurité des applications

1. Les entrées des utilisateurs doivent être contrôlées et filtrées avant traitement (longueur, type de données attendues, etc.) ;
2. Seules les données correspondant à des paramètres attendus doivent être prises en compte;
3. Toute donnée reçue par le composant serveur d'une application doit, avant d'être transmise à une ressource utilisatrice (navigateur internet, moteur de base de données, moteur applicatif, etc.) soit :
   - Expurgée des éléments pouvant être interprétés ou exécutés ;
   - Rendue non interprétable.
4. L'accès d'une application à une base de données doit se faire avec un compte spécifique bénéficiant des privilèges strictement nécessaires et suffisants ;
5. Le compte d'administrateur de base de données ne doit jamais être utilisé pour accéder à une base de données depuis un programme (une application) non dédié à son administration ;

6. Les références des objets internes - fichiers, répertoires, enregistrements de bases de données, etc., ne doivent pas être exposés directement à des tiers ;
7. Lorsque les données sensibles temporaires ne peuvent être protégées par un contrôle d'accès adéquat, elles doivent être chiffrées par un algorithme robuste et fiable, validé par le Directeur des Systèmes d'Information (DSI) ;
8. Tout message d'erreur technique présenté à l'utilisateur doit être personnalisé de façon à ne pas divulguer d'information sur les composants techniques sous-jacents ;
9. Le message d'erreur présenté à l'utilisateur suite à un échec d'authentification ne doit pas fournir d'information relative à la raison de cet échec ;
10. Toute application Internet et toute application sensible doit faire l'objet d'un audit de sécurité avant sa mise en production ;
11. Le code source doit être nettoyé des éléments de test, et des débogages avant toute mise en production ;
12. Le code source et les éléments associés au développement (spécifications, programmes de vérification et de validation, documentation) doivent être considérés comme actifs sensibles et gérés comme tels.

XII. Politiques de gestion des incidents liés à la sécurité de l'information

1. Les événements liés à la sécurité de l'information doivent être signalés/rapportés, dans les meilleurs délais, à travers les voies hiérarchiques appropriées de la CNSSAP ;
2. La CNSSAP doit mettre en place une procédure formelle permettant de garantir une réponse rapide, efficace et pertinente en cas d'incidents liés à la sécurité de l'information et occasionnant des perturbations des activités de l'instance ;
3. Pour réduire la probabilité ou l'impact d'incident ultérieur, les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées ;
4. Tous les utilisateurs du système d'information de la CNSSAP, doivent dans les meilleurs délais, signaler à la Direction des Systèmes d'Information, les failles de sécurité rencontrées, afin d'éviter tout incident lié à la sécurité de l'information ;
5. Après un incident de la sécurité de l'information, les preuves doivent être collectées, conservées et présentées en cas de besoin conformément aux dispositions internes, légales et réglementaires de la CNSSAP ;
6. Un plan de continuité d'activité informatique doit être établi en tenant compte des exigences de disponibilité des ressources et de la continuité des services et moyens informatiques et réseaux ;
7. Le plan de continuité d'activité doit être périodiquement testé, au moins une fois par an, afin que le personnel concerné comprenne toutes les dispositions du plan ;
8. Tout le personnel concerné doit être sensibilisé au plan de continuité d'activité informatique et doit comprendre son rôle dans ce plan ;
9. Les systèmes d'informations critiques de la CNSSAP doivent être capables de supporter des catastrophes et sinistres mineurs (coupure d'alimentation, crash d'un disque dur, etc.) ;
10. Tous les systèmes et applications critiques pour la continuité d'activité doivent être récupérables/ restaurables dans un temps raisonnable ;

11. Pour répondre aux exigences de disponibilités, des moyens de traitement de l'information doivent être mis en place avec suffisamment de redondances.

XIII. Politiques à suivre pour le respect de la conformité

1- Le Chef de Département Sécurité des Systèmes d'Information (CDSSI) doit élaborer des revues périodiques des logiciels utilisés au sein de la CNSSAP et installés sur les ordinateurs, portables, serveurs ou autre type d'équipement. Il doit s'assurer que tous les logiciels installés disposent d'une licence logicielle pour l'exploitation. Tous les logiciels qui ne disposent pas de licences doivent être immédiatement désinstallés et supprimés ;
2- La CNSSAP s'engage à se conformer complètement aux exigences légales de la protection des données à caractère personnel (Titre III de l'ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique en RDC).

XIV. Politique de gestion des risques informatiques

1- L'objectif de cette politique est d'établir un cadre formel pour identifier, évaluer et gérer les risques informatiques au sein de l'établissement. Elle vise à assurer la disponibilité, l'intégrité et la confidentialité des informations critiques, ainsi qu'à minimiser les interruptions potentielles des activités ;
2- Tous les employés sont responsables de signaler les incidents de sécurité et de coopérer dans l'application de cette politique ;
3- Les risques informatiques potentiels doivent être identifiés et évalués annuellement lors de la revue de la cartographie des risques ;
4- Un inventaire des actifs informatiques, y compris les données sensibles, doit être maintenu et mis à jour régulièrement ;
5- Des évaluations annuelles des vulnérabilités, des menaces externes et internes doivent être effectuées ;
6- Des contrôles de sécurité appropriés doivent être mis en place pour atténuer les risques identifiés ;
7- En cas de risques élevés, des plans d'action spécifiques doivent être élaborés et mis en œuvre ;
8- Des programmes de sensibilisation réguliers sur la sécurité informatique doivent être dispensés à tous les employés ;
9- Les employés doivent être informés des politiques et des procédures de sécurité et des conséquences du non-respect ;
10- Un plan de continuité d'activités doit être établi pour minimiser l'impact des incidents de sécurité sur les opérations ;
11- Des exercices de simulation réguliers doivent être effectués pour tester l'efficacité du plan ;
12- Cette politique doit être révisée périodiquement pour s'assurer qu'elle reste en phase avec l'évolution des risques informatiques et des technologies ;
13- Les modifications doivent être communiquées à tous les employés concernés ;

14- En acceptant les politiques de gestion des risques informatiques, les employés reconnaissent leur responsabilité dans la protection des actifs informatiques de l'établissement.

XV. Politique de développement des applications

1- Cette politique vise à établir les normes et les directives pour le développement d'applications afin d'assurer la qualité, la sécurité et la cohérence à travers l'ensemble de notre organisation ;
2- Toutes les applications doivent suivre un processus de développement standard, comprenant les phases de conception, de développement, de test et de déploiement ;
3- Les développeurs doivent intégrer des mesures de sécurité dès la conception. Les vulnérabilités identifiées doivent être corrigées immédiatement ;
4- Les applications doivent respecter les normes de codage et les directives d'interface utilisateur établies ;
5- Toutes les applications doivent être conformes aux réglementations et aux politiques de confidentialité en vigueur au niveau national ;
6- Chaque application doit être accompagnée d'une documentation complète, y compris des cahiers des charges et des guides d'utilisation ;
7- Toutes les applications doivent subir des tests approfondis avant le déploiement ;
8- Le Chef de Département Sécurité des Systèmes d'Information (CDSSI) doit vérifier le respect de différentes étapes de développement des applications en interne ;
9- L'utilisation d'un système de gestion de versions doit être de mise pour garantir la traçabilité des changements ;
10- Les mises à jour régulières et la maintenance sont cruciales pour assurer la sécurité et la performance des applications ;
11- La communication efficace entre les équipes de développement, les parties prenantes et les utilisateurs finaux est essentielle ;
12- Une évaluation annuelle des processus de développement permettra d'identifier les opportunités d'amélioration ;
13- Cette politique est sujette à révision et doit être respectée par tous les membres de l'équipe de développement d'applications.

XVI. Politique de classification de l'information

1- Cette politique vise à établir des normes pour la classification appropriée de l'information afin de garantir la confidentialité, l'intégrité et la disponibilité des données au sein de notre établissement ;
2- Une information **confidentielle** est une information critique nécessitant le plus haut niveau de protection. L'accès est limité aux personnes autorisées uniquement ;
3- Une information **intermédiaire** est une information nécessitant une protection modérée. L'accès est restreint à des groupes spécifiques définis ;
4- Une information **publique** est non confidentielle et accessible à l'ensemble de l'établissement et, dans certains cas, au public ;

5- Chaque employé est responsable de classer correctement l'information qu'il manipule en fonction des directives établies ;
6- Le Chef de Département Sécurité des Systèmes d'Information (CDSSI) est chargé de sensibiliser les employés sur l'importance de la classification de l'information ;
7- Un processus clair de classification doit être suivi lors de la création ou de la manipulation d'informations sensibles ;
8- Les critères de classification doivent être définis et communiqués à tous les employés ;
9- Les mesures de sécurité appropriées doivent être mises en place en fonction de la classification de l'information ;
10- L'accès à l'information doit être strictement contrôlé en fonction des niveaux de classification ;
11- Tous les employés doivent recevoir une formation régulière sur les politiques de classification et sensibilité de l'information ;
12- Les classifications existantes doivent être réévaluées en cas de changement de statut ou de nature de l'information.

XVII. Politique de Sauvegarde de Données

1- Cette politique vise à assurer la protection et la disponibilité des données critiques de l'institution en établissant des procédures de sauvegarde appropriées ;
2- Cette politique s'applique à toutes les données stockées, traitées ou transmises par l'institution, qu'elles soient électroniques ou physiques ;
3- La Direction des Systèmes d'Information est chargée de mettre en œuvre et de gérer les systèmes de sauvegarde ;
4- Chaque employé est responsable de la sauvegarde régulière dans SHARE des données qu'il génère ou manipule ;
5- Les sauvegardes complètes sont effectuées hebdomadairement ;
6- Les sauvegardes différentielles sont effectuées quotidiennement ;
7- Les sauvegardes incrémentielles sont effectuées une ou plusieurs fois par jour ;
8- Les données sont sauvegardées sur des serveurs sécurisés, des dispositifs de stockage externes ou dans le cloud ;
9- Toutes les sauvegardes sont cryptées pour assurer la confidentialité des données ;
10- Des tests de restauration sont effectués régulièrement pour garantir la fiabilité des sauvegardes ;
11- Les résultats des tests sont documentés et conservés à des fins d'audit ;
12- Les données sensibles sont conservées plus longtemps que les données non sensibles ;
13- Les sauvegardes sont stockées dans des lieux sécurisés, à l'abri des catastrophes naturelles et des accès non autorisés ;
14- Des copies de sauvegarde sont stockées hors site pour réduire les risques de perte de données en cas de sinistre ;
15- Tous les employés doivent être formés sur les procédures de sauvegarde et de récupération des données.

XVIII. Politique BYOD (Bring Your Own Device)

1- La politique BYOD a pour but de définir les règles et les responsabilités associées à l'utilisation des appareils personnels au sein de la CNSSAP. Elle vise à établir des normes de sécurité et de confidentialité pour protéger les données de l'institution et à garantir une utilisation responsable des dispositifs personnels ;
2- Cette politique s'applique à tous les employés et parties prenantes qui utilisent leurs propres appareils (smartphones, tablettes, ordinateurs portables, etc.) pour accéder aux ressources de l'institution ;
3- Les appareils doivent être équipés de logiciels antivirus et de pare-feu à jour ;
4- Les employés sont tenus de déclarer immédiatement la perte ou le vol de leur appareil à l'équipe informatique ;
5- Les données professionnelles doivent être stockées uniquement dans des applications et des espaces sécurisés approuvés par l'institution ;
6- L'accès au réseau depuis des appareils personnels doit se faire par le biais de connexions sécurisées, telles que des VPN ;
7- Les dispositifs non conformes aux normes de sécurité seront exclus de l'accès au réseau ;
8- Les employés doivent accepter l'installation d'applications de gestion des appareils pour garantir la conformité aux politiques de sécurité ;
9- L'institution se réserve le droit d'effacer les données professionnelles à distance en cas de perte, de vol, ou de cessation d'emploi ;
10- Les employés sont responsables de la sécurité de leurs appareils et doivent signaler tout incident de sécurité à l'équipe informatique ;
11- Les utilisateurs doivent respecter toutes les lois et réglementations en vigueur, y compris celles relatives à la confidentialité des données ;
12- Les appareils doivent être sécurisés par un mot de passe de niveau moyen, au minimum ;
13- Les employés doivent s'assurer que leurs appareils sont verrouillés lorsqu'ils ne sont pas utilisés pour éviter tout accès non autorisé ;
14- Les employés doivent respecter la politique de sécurité de la CNSSAP et ne pas divulguer d'informations sensibles ou confidentielles à partir de leurs appareils personnels ;
15- Les employés de la CNSSAP sont responsables de la maintenance et du support technique de leurs propres appareils ;
16- La CNSSAP ne fournira pas de support technique pour les appareils personnels de ses employés ;
17- La CNSSAP respecte la vie privée des employés et ne collectera que les données nécessaires à des fins professionnelles ;
18- Les employés sont encouragés à séparer clairement les données professionnelles et personnelles sur leurs appareils ;
19- La CNSSAP se réserve le droit de révoquer les privilèges BYOD si un employé viole cette politique ou compromet la sécurité des données de l'institution.

XIX. Politique de réplication de Données

1- La politique de réplication de données vise à assurer la disponibilité, la redondance et la résilience des données de l'institution en mettant en place des procédures de réplication régulières et sécurisées ;
2- Cette politique s'applique à toutes les données critiques de l'institution, qu'elles soient stockées sur site, dans le cloud ou dans d'autres emplacements distants ;
3- La direction des systèmes d'information est responsable de la conception, de la mise en œuvre et de la gestion des solutions de réplication de données ;
4- Le Chef de Département Systèmes, Réseaux et Sécurité est responsable de surveiller et de maintenir les systèmes de réplication en bon état de fonctionnement ;
5- Les stratégies de réplication sont adaptées en fonction de la classification des données ;
6- La réplication synchrone est utilisée pour les données critiques nécessitant une redondance en temps réel. Cela garantit que toutes les modifications sont répliquées immédiatement sur les sites de secours ;
7- La réplication asynchrone est utilisée pour les données moins critiques, permettant un délai acceptable entre les modifications sur le site principal et leur réplication sur le site de secours ;
8- La fréquence de réplication est déterminée en fonction de la criticité des données, de la bande passante disponible et des exigences de récupération après sinistre ;
9- Les données critiques peuvent être répliquées en continu ou à intervalles réguliers, tandis que les données moins critiques peuvent être répliquées moins fréquemment ;
10- Les données répliquées doivent être protégées en transit et au repos en utilisant des protocoles de cryptage ;
11- Les accès aux données répliquées doivent être restreints et contrôlés pour empêcher tout accès non autorisé ;
12- Des tests réguliers de récupération sont effectués pour vérifier la capacité des systèmes de réplication à restaurer les données en cas de sinistre ou de panne ;
13- Les résultats des tests sont documentés et analysés pour identifier et résoudre les éventuels problèmes.

XX. Politique de gestion des mots de passe

1- Le mot de passe comporte 7 caractères alphanumériques au minimum (combinaison des lettres, chiffres, et caractères spéciaux) ;
2- Chaque utilisateur dans le domaine est tenu de modifier son mot de passe selon la fréquence de 60 jours ;
3- En cas d'oubli de mot de passe, l'utilisateur sollicite le changement du mot de passe auprès de la Direction des Systèmes d'Information ;
4- Les anciens mots de passe ne doivent pas être réutilisés ;
5- Aucun utilisateur ne peut faire usage du mot de passe d'un tiers ;
6- L'authentification à deux facteurs doit être activée lorsque cela est possible, pour ajouter une couche supplémentaire de sécurité ;

7- Les utilisateurs doivent être sensibilisés aux bonnes pratiques de gestion des mots de passe, y compris l'importance de choisir des mots de passe forts et de ne pas les partager avec d'autres personnes ;
8- Les mots de passe partagés (administrateur, système etc.) doivent être gérés de manière sécurisée, en limitant l'accès aux personnes autorisées et en les changeant régulièrement ;
9- Les mots de passe doivent être stockés de manière sécurisée à l'aide de méthodes de hachage et de chiffrement robustes ;
10- Les systèmes doivent être configurés pour bloquer ou limiter le nombre de tentatives de connexion infructueuses par mot de passe.

ANNEXE : Glossaire et Terminologies

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

- **Bien/actif « assets » :** Tout élément représentant de la valeur pour l'organisme [ISO/CEI 13335-5].
- **Mesure « control » :** Moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices et les pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique. Le terme « mesure » est également utilisé comme synonyme de « conservation » ou de « contre-mesure ».
- **Moyens de traitement de l'information :** Tout(e) système, service ou infrastructure de traitement de l'information, ou locaux les abritant.
- **Sécurité de l'information :** Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées.
- **Événement lié à la sécurité de l'information :** Occurrence identifiée d'un état d'un système, d'un service ou d'un réseau, indiquant une brèche possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité [ISO/IEC 27035- 2 : 2016].
- **Incident lié à la sécurité de l'information :** Un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information [ISO/IEC 27035- 2 : 2016].
- **Politique :** Intentions et dispositions générales formellement exprimées par la direction.
- **Risque :** Combinaison de la probabilité d'un événement et de ses conséquences [ISO/IEC27005 :2011].
- **Analyse du risque :** Utilisation systématique d'informations pour identifier les sources et pour estimer le risque [ISO/IEC27005 :2011].
- **Tiers :** Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.
- **Menace :** Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme [ISO/IEC27005 :2011].
- **Vulnérabilité :** Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace [ISO/IEC27005 :2011].
- **Disponibilité :** Etat qui caractérise un système ou une ressource lorsque les utilisateurs disposant des autorisations nécessaires peuvent y accéder et l'utiliser à la demande. La disponibilité est l'une des caractéristiques principales d'un système sécurisé.
- **Confidentialité :** Propriété d'une information qui n'est ni rendue disponible, ni divulguée aux personnes, aux entités ou aux processus non autorisés [ISO/IEC27005 :2011].

- **Intégrité :** Propriété d'une information qui n'a été ni modifiée, ni détruite de façon non autorisée [ISO/IEC27005 :2011].
- **Probabilité :** Possibilité qu'un événement se produise.
- **Impact :** Pertes commerciales globales à prévoir en cas d'exploitation par un agent menaçant d'une vulnérabilité à l'encontre d'une ressource.
- **Ligne directrice :** Description clarifiant ce qu'il convient de réaliser et par quels moyens, en vue d'atteindre les objectifs fixés par la politique de l'organisme [ISO/CEI 13335- 5].