PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE DE COTE D'IVOIRE
Union – Discipline – Travail

DECRET N° 2021-915 DU 22 DECEMBRE 2021 PORTANT ADOPTION DE LA POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ADMINISTRATION PUBLIQUE

LE PRESIDENT DE LA REPUBLIQUE,

Sur rapport du Ministre de l'Economie Numérique, des Télécommunications et de l'Innovation,

Vu la Constitution ;

Vu la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;

Vu la loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;

Vu la loi n° 2017-803 du 07 décembre 2017 d'orientation de la Société de l'Information en Côte d'Ivoire ;

Vu l'ordonnance n° 2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

Vu l'ordonnance n° 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n°2018-875 du 22 novembre 2018 portant organisation et fonctionnement de la Commission Nationale du Développement de la Société de l'Information ;

Vu le décret n° 2021-176 du 26 mars 2021 portant nomination du Premier Ministre, Chef du Gouvernement ;

Vu le décret n° 2021-181 du 06 avril 2021 portant nomination des Membres du Gouvernement ;

Vu le décret n° 2021-190 du 28 avril 2021 portant attributions des Membres du Gouvernement ;

Vu le décret n° 2021-464 du 08 septembre 2021 portant organisation du Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation ;

LE CONSEIL DES MINISTRES ENTENDU,

DECRETE :

Article 1 : Est adoptée la Politique de Sécurité des Systèmes d'Information de l'Administration publique, en abrégé PSSI, annexée au présent décret.

Article 2 : Les organismes publics sont tenus de se conformer à la PSSI.

Article 3 : Le Ministre chargé de l'Economie Numérique procède par arrêté à la révision de la PSSI, chaque fois que de besoin.

Article 4: Le Ministre de l'Economie Numérique, des Télécommunications et de l'Innovation est chargé de l'exécution du présent décret qui sera publié au *Journal Officiel* de la République de Côte d'Ivoire.

Fait à Abidjan, le 22 décembre 2021

Alassane OUATTARA

Copie certifiée conforme à l'original
Le Secrétaire Général du Gouvernement

RÉPUBLIQUE DE CÔTE D'IVOIRE
SECRETARIAT GENERAL DU GOUVERNEMENT

Eliane Attè BIMANAGBO
Préfet

PRESIDENCE DE LA REPUBLIQUE

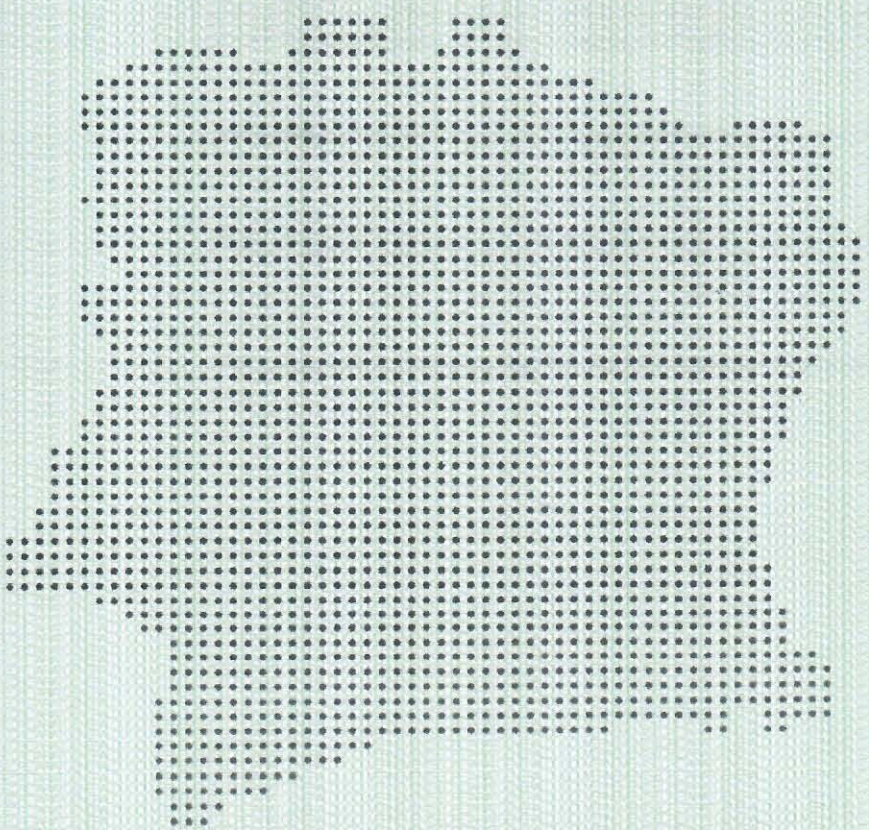
REPUBLIQUE DE COTE D'IVOIRE
Union – Discipline – Travail

ANNEXE AU DECRET N° 2021-915 DU 22 DECEMBRE 2021 PORTANT ADOPTION DE LA POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ADMINISTRATION PUBLIQUE

UNION – DISCIPLINE – TRAVAIL

REPUBLIQUE DE CÔTE D'IVOIRE

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ADMINISTRATION PUBLIQUE



GESTION DOCUMENTAIRE			
Titre		*Politique de Sécurité des Systèmes d'Information de l'Administration Publique*	
Version		*1.0*	
Classification		*Diffusion Restreinte*	
Créé par		*Comité interministériel de rédaction PSSI*	
Date de publication		*09/06/2021*	
HISTORIQUE DES MODIFICATIONS			
Date	*version*	*Créé par*	*Description de la modification*
		PSSI	

TABLE DES MATIERES

PREAMBULE

Les services offerts par l'administration publique aux citoyens via les télécommunications et les technologies de l'information (TIC) sont en nette progression en Côte d'Ivoire, depuis la dernière décennie. De nombreux projets structurants de l'administration sont mis en œuvre, afin de renforcer la facilité d'accès, la transparence du traitement, la fiabilité et l'efficacité des services publics.

L'ouverture grandissante des systèmes d'information sur internet est le signe de la vitalité du secteur des TIC en Côte d'Ivoire. Toutes les entreprises, privées mais aussi publiques ont pris conscience des enjeux de la dématérialisation dans leurs stratégies respectives de développement et de production.

Cependant, bien qu'ils apportent un gain de productivité inégalé jusqu'ici par d'autres innovations, l'usage des plateformes numériques, des sites web, des réseaux informatiques et applications web n'est pas sans risques pour les nombreuses entreprises qui les exploitent, notamment les administrations publiques.

Des sites web peuvent être la cible d'attaques informatiques et être défigurées et par conséquent, ternir l'image et la crédibilité des administrations publiques ivoiriennes. De plus, des services et procédures administratives peuvent être bloqués du fait de l'indisponibilité des réseaux et de l'internet.

La mise en œuvre des mesures organisationnelles et techniques de gestion des risques et de sécurisation des systèmes d'information est une nécessité quasi-vitale pour des entités, organisations possédant ou opérant des actifs sensibles, telles que les services de l'Etat (départements ministériels, administration, collectivités territoriales, etc.).

La Politique de Sécurité des Systèmes d'Information (PSSI) est un cadre de référence pour la mise en œuvre de mesures de protection applicables aux systèmes d'information de l'Etat. Elle décrit une démarche globale de protection des systèmes d'information de l'Etat, applicable par l'ensemble des administrations et entreprises publiques de Côte d'Ivoire pour prévenir et faire face aux cybermenaces. Cependant, elle peut servir de lignes directrices à toutes les organisations pour la mise en œuvre d'une stratégie globale de sécurisation de leurs systèmes d'information.

Elle est élaborée sur la base du Référentiel Général de Sécurité des Systèmes d'Information (RGSSI), en définissant des mesures techniques et organisationnelles qui constituent un socle minimal. Dans certains cas, les entités concernées devront s'appuyer sur la PSSI, les normes applicables et les guides y relatifs pour élaborer des mesures détaillées et plus spécifiques à leurs contextes respectifs.

PREMIERE PARTIE :

DISPOSITIONS GENERALES

1) CHAMPS D'APPLICATION

La PSSI est une déclinaison opérationnelle du référentiel général de sécurité des systèmes d'information et s'adresse à l'ensemble des composantes du système d'information (moyens humains, techniques, organisationnels, quels que soit leurs lieux d'implantation) de l'Etat, notamment celui des :

- Ministères ;
- Institutions ;
- Autorités administratives ;
- Etablissements publics et entités sous-tutelles (agences, centres nationaux, bureaux d'études...) ;
- Collectivités territoriales ;
- Etc.

Elle s'applique de ce fait, à tous les personnels autorisés à accéder à tout ou partie du système d'information, les fournisseurs de biens et services, les contractuels, les matériels et logiciels faisant partie du système d'information. Plus spécifiquement, elle est adressée aux responsables de la sécurité du système d'information (RSSI) au sein des entités d'Etat, les directeurs des systèmes d'information (DSI), les référents techniques et chargés de la sécurité et de l'exploitation de systèmes d'information.

2) OBJECTIFS

La PSSI est un outil de pilotage stratégique de la sécurité, à travers une approche globale de gestion des risques, qui vise entre autres :

- Le développement d'une culture de gestion et de maîtrise des risques des systèmes d'information ;
- La mise en place à tous les niveaux de l'Etat et au sein de chaque administration publique d'une organisation destinée à assurer la sécurité et la défense des systèmes d'information ;
- L'établissement d'un rapport annuel sur l'état de la sécurité des systèmes d'information avec une synthèse de la cartographie des systèmes d'information et leur niveau de maturité en sécurité ;
- La sensibilisation et la formation des autorités administratives à la sécurité des systèmes d'information ;
- La définition de politiques internes de sécurité des systèmes d'information basées sur la politique nationale de sécurité ;
- L'harmonisation des pratiques de gestion de la sécurité de l'information au sein de services de l'Etat.

3) MODALITES DE MISE EN APPLICATION DE LA PSSI

La PSSI entre en vigueur le jour de sa publication.

L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire assure la fonction d'autorité nationale chargée de veiller à la sécurité des systèmes d'information, conformément aux dispositions de la Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques. A ce titre, elle définit les mesures à mettre en œuvre pour la protection des systèmes d'information, gérer et coordonner les actions de gestion des incidents de sécurité informatique impactant les systèmes d'informations des services de l'Etat à travers le CI-CERT (Côte d'Ivoire-CERT) et protéger les infrastructures critiques nationales. Par ailleurs, elle coordonne les actions de contrôle de la mise en œuvre de la PSSI et du maintien du niveau de sécurité des systèmes d'information de l'Etat.

Au niveau de chaque service de l'Etat, la responsabilité de la mise en œuvre de la PSSI est du ressort du comité sécurité de l'information (CSI). Il met tout en œuvre pour fournir les moyens nécessaires à la mise en œuvre PSSI au niveau de son organisation et vérifie la mise en œuvre effective des dispositions de la PSSI. Ce comité est appuyé par un acteur opérationnel assurant la fonction de responsable de la sécurité des systèmes d'information (RSSI).

Le RSSI définit en fonction des besoins, une chaine opérationnelle d'acteurs composée d'analystes de sécurité des systèmes d'information (ASSI).

Sous la responsabilité du CSI, le RSSI établit annuellement, un bilan annuel de la sécurité des SI, comportant à minima :

- Une synthèse de la cartographie des SI et de ses mises à jour (conformément au plan d'urbanisation des systèmes d'information de l'Etat) ;
- Des indicateurs permettant d'appréhender la maturité en SSI ;
- Un récapitulatif des actions réalisées pour la mise en conformité à la PSSI ;
- Un récapitulatif des incidents de sécurité des systèmes d'information constatés (accompagnés éventuellement de descriptifs des dispositions mises en œuvre pour les résoudre).

4) CONTROLE ET MAINTENANCE DE LA PSSI

L'ARTCI assure le contrôle de la mise en application de la PSSI au sein des services de l'Etat. A cet effet, elle effectue des audits de sécurité des systèmes d'information des services de l'Etat. Ces audits peuvent porter sur les aspects organisationnels ou techniques de la sécurité de l'information au sein de l'organisation ou sur les deux aspects simultanément.

Les contrôles de conformité peuvent être réalisés de manière inopinée selon les besoins, à la suite de graves incidents de sécurité ou en cas de suspicion de fortes insuffisances dans la sécurité.

5) GESTION DES INCIDENTS ET GESTION DE CRISE

Une stratégie de réponse rapide et efficace aux incidents de sécurité des systèmes d'information est mise en place, afin de réagir promptement et contenir les impacts des incidents de sécurité sur le plan national.

Tout utilisateur du système d'information d'une entité d'Etat doit signaler immédiatement, les faits ou événements susceptibles d'affecter ou ayant affecté la sécurité du système d'information auquel il a accès ou duquel il a eu connaissance. L'utilisateur signale l'incident au responsable de la sécurité des SI (RSSI) par le biais des analystes de sécurité des SI (ASSI).

En cas de graves incidents, ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou la traçabilité du système d'information, le responsable de la sécurité du système d'information remonte sans délais, l'alerte au CERT national. Les alertes peuvent être transmises par un analyste de sécurité des systèmes d'information, sous le contrôle de son RSSI.

Côte d'Ivoire Computer Emergency Response Team (CI-CERT) est le centre national de veille, de réponse, gestion et de coordination du traitement des incidents de sécurité des systèmes d'information.

En cas de grave crise, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire met en œuvre un plan de coordination en relation avec l'ensemble des RSSI des services de l'Etat.

DEUXIEME PARTIE :

PRINCIPES ET REGLES DE SECURITE

1) LEADERSHIP & GOUVERNANCE DE LA SECURITE DE L'INFORMATION

Leadership et engagement du top management

Objectif :

- *Faire preuve de leadership et affirmer l'engagement des plus hautes instances dirigeantes des entités d'Etat en faveur de la sécurité des systèmes d'information.*

Règles

1) Le ministre en charge de chaque département ministériel, le Président d'institution adopte et signe une politique générale de sécurité des systèmes d'information. Cette politique symbolise l'engagement de la plus haute hiérarchie au sein de l'entité, à faire la promotion de la sécurité de l'information.
2) La politique générale de sécurité de l'information est affichée de manière visible aux entrées et dans les locaux des bâtiments de chaque entité.

Politiques spécifiques de sécurité de l'information

Objectif :

- *Formaliser les règles, pratiques et procédures de gestion de la sécurité de l'information et d'utilisation des ressources TIC mises à disposition des usagers.*

Règles

1) Le comité sécurité de l'information définit un ensemble de politiques en matière de sécurité de l'information qui soient approuvées par la direction, diffusées et communiquées aux agents et aux tiers concernés.
2) La politique générale de sécurité est appuyée par un ensemble de politiques spécifiques, en fonction des besoins et du contexte de l'entité. Sans s'y limiter, les politiques ci-après peuvent être abordées :
    a. Le contrôle d'accès ;
    b. La classification (et le traitement) de l'information ;
    c. La sécurité physique et environnementale ;
    d. Utilisation correcte des actifs ;
    e. Bureau propre et écran vide ;
    f. Transfert de l'information ;
    g. Appareils mobiles et télétravail ;
    h. Restrictions en matière d'installation et d'utilisation de logiciels ;
    i. Sauvegarde ;
    j. Transfert de l'information ;

k. Protection contre les logiciels malveillants ;
l. Gestion des vulnérabilités techniques ;
m. Mesures de sécurité cryptographiques ;
n. Sécurité des communications ;
o. Protection de la vie privée et des informations personnelles identifiables ;
p. Relations avec les fournisseurs.

3) Le Référentiel Général de Sécurité des Systèmes d'Information définit une liste complète des politiques applicables pour la sécurité de l'information. Le RSSI de chaque entité élabore et met en œuvre les politiques applicables à son contexte.
4) Sous approbation du comité sécurité de l'information, le Responsable de la Sécurité de l'Information (RSSI) désigne un propriétaire de chaque politique spécifique.
5) Le responsable d'une politique spécifique est chargé d'effectuer une revue périodique programmée ou en cas de changements majeurs dans le contexte de l'entité, afin de l'adapter au mieux aux besoins de sécurité.
6) La revue comporte une appréciation des possibilités d'amélioration de la politique de l'organisation et une approche de management de la sécurité de l'information pour répondre aux changements intervenant dans l'environnement organisationnel, aux circonstances liées à l'activité, au contexte juridique ou à l'environnement technique.
7) Chaque fois qu'une politique spécifique est modifiée, elle fait l'objet d'une approbation par le comité sécurité de l'information.

2) ORGANISATION DE LA SECURITE DE L'INFORMATION

Fonctions et responsabilités liées à la sécurité de l'information

Objectifs

- *Mettre en place une organisation et un schéma de gouvernance clair et approuvé, afin de gérer la sécurité de l'information au sein de l'entité.*

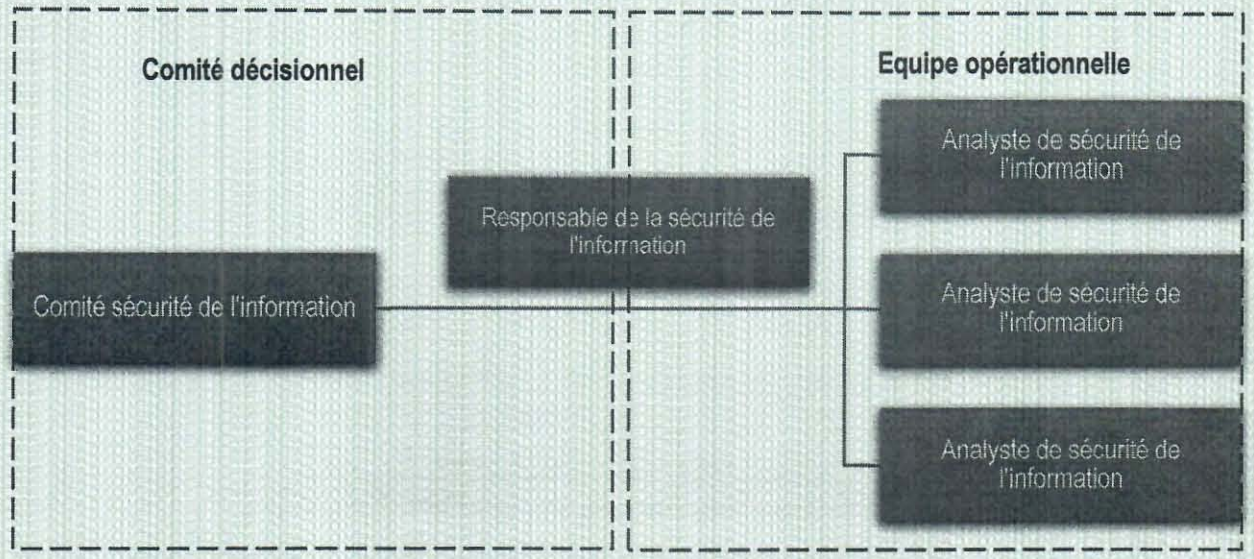


Schéma de gouvernance de la sécurité de l'information

Règles

1) Chaque entité met en place une organisation spécifique distincte des équipes informatiques pour la gestion de la sécurité de l'information, tel que présenté dans le schéma de gouvernance ci-dessus. L'organisation de la sécurité de l'information est composée de :

Comité sécurité de l'information (CSI) :

Le comité sécurité de l'information (CSI) est un comité stratégique composé de personnes responsables de la protection du patrimoine informationnel de l'entité. Il est constitué au moins de :

- *Ministre ou Président du Conseil d'Administration ou Président*
- *Directeur Général*
- *Conseiller technique en charge des TIC*
- *Directeur en charge des ressources humaines (DRH)*
- *Directeur en charge des affaires financières (DAF)*
- *Directeur en charge des Affaires juridiques (DAJU)*

- *Directeur en charge des Systèmes d'Information (DSI)*
- *Responsable de la sécurité de l'information (RSSI)*
- *Représentant du personnel*

En fonction des besoins et du contexte de chaque entité des personnes ressources compétentes peuvent être rajoutées au comité sécurité de l'information.

Le CSI est chargé de définir, approuver et communiquer la politique de sécurité de l'information et les politiques spécifiques associées.

Le CSI promeut, planifie et s'assure de la bonne mise en œuvre des mesures adéquates en matière de sécurité de l'information au sein de l'entité.

Le CSI s'assure de mettre à disposition toutes les ressources nécessaires à la mise en œuvre de la politique de sécurité de l'information et prendre en compte les changements non prévus ayant un impact sur la sécurité de l'information.

Responsable sécurité de systèmes d'information (RSSI)

Le Responsable de Sécurité de l'Information (RSSI) est désigné pour ses compétences en gestion de la sécurité de l'information.

Le RSSI est désigné formellement par un acte administratif approuvé et signé par le premier responsable de l'entité. La décision formelle comprend une fiche de poste, définissant clairement les rôles, missions et champs de compétences de son ressort.

Le RSSI a pour rôle de veiller à la sécurité des systèmes d'information au sein de l'entité, en s'alignant sur les orientations stratégiques définies par le comité sécurité de l'information. Il assure la coordination des actions nécessaires pour la mise en œuvre de la politique de sécurité de l'information.

Il assure la gestion quotidienne de la fonction sécurité et pilote la stratégie de l'entité en matière de sécurité de l'information. Il est le point focal de l'entité pour les échanges avec l'extérieur et s'assure à ce titre de développer un réseau de contact et des liens de collaboration avec les entités externes compétentes et utiles à l'accomplissement de ses missions.

Analyste de sécurité des systèmes d'information (ASSI)

Les analystes de sécurité des systèmes d'information (ASSI) assurent la responsabilité de la sécurité dans leurs périmètres techniques respectifs. Ils veillent au quotidien à la mise en œuvre des moyens et procédures techniques dans leur domaine de compétence.

Les fonctions assurées par les ASSI peuvent inclure sans y être limitées : sécurité réseaux, sécurité applicative, gestion d'incidents, testeur d'intrusions, veille technique (faille, vulnérabilités, etc.).

Les équipes informatiques peuvent assurer des fonctions de sécurité opérationnelle des systèmes d'information. Dans ces cas, un pôle sécurité est dédié à la sécurité de l'information au sein de l'équipe informatique.

Relations avec les acteurs extérieurs

Objectifs

- *Entretenir des relations appropriées avec les autorités compétentes sur le plan national et international, des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles.*

Règles

1) Le RSSI est le point focal de l'entité en matière de sécurité de l'information. Il établit des liens formels de coopération avec les autorités nationales compétentes en matière de cybersécurité, protection des données à caractère personnel et lutte contre la cybercriminalité. A ce titre, il établit un moyen de communication et d'échanges sécurisés avec l'ARTCI, le CI-CERT, la plateforme de lutte contre la cybercriminalité (PLCC), la Direction de l'Informatique et des Traces Technologiques (DITT).
2) Le RSSI établit des liens de coopération, en vue de mieux connaître les bonnes pratiques et se tenir informé de l'évolution des savoirs relatifs à la sécurité, s'assurer que la connaissance de l'environnement de la sécurité de l'information est à jour et exhaustive et recevoir rapidement des alertes, des conseils et des correctifs logiciels portant sur les attaques et les vulnérabilités.
3) Il envisage et coordonne l'établissement d'accords de partage de l'information avec les groupes, forums spécialisés et association de professionnels de la sécurité de l'information en vue d'améliorer la coopération et la coordination dans le domaine de la sécurité.

3) GESTION DES RISQUES LIES A LA SECURITE DU SYSTEME D'INFORMATION

Objectifs :

- *Tenir compte des enjeux et des exigences, et déterminer les risques et opportunités qui nécessitent d'être abordés pour sécuriser son système d'information*
- *définir et appliquer un processus d'appréciation des risques de sécurité de l'information*
- *définir et appliquer un processus de traitement des risques de sécurité de l'information*
- *établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information*

Règles

1) Le comité sécurité de l'information définit les résultats escomptés en matière de gestion des risques de sécurité de l'information en tenant compte des enjeux et des exigences auxquelles est soumise l'entité. Il approuve les actions menées pour traiter les risques et opportunité, la manière d'intégrer et de mettre en œuvre les actions au sein des processus pour garantir la sécurité de l'information et la manière d'évaluer l'efficacité de ces actions.
2) L'entité élabore sous la conduite du RSSI, une étude globale des risques de sécurité de l'information. Cette étude est documentée et comprend un résumé des activités suivantes :
    a. critères de risque de sécurité de l'information incluant les critères d'acceptation des risques et les critères de réalisation des appréciations des risques de sécurité de l'information
    b. identification des risques de sécurité de l'information
    c. analyse des risques (conséquences potentielles, vraisemblance de l'occurrence, niveaux)
    d. évaluation des risques incluant la priorisation des risques identifiés en fonction des critères de risques établis
    e. Plan d'action des mesures à mettre en œuvre pour traiter les risques identifiés.
3) Le RSSI est responsable de documenter et conserver cette étude qui est effectuée au moins annuellement ou en cas de graves incidents ou changements du contexte ou de l'environnement de l'entité.
4) Les plans d'action définis dans le cadre de l'étude des risques sont formellement approuvés par le comité sécurité de l'information (CSI).

4) SECURITE DES RESSOURCES HUMAINES

Objectifs :

- *S'assurer que les agents, salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.*
- *Mettre l'humain au cœur de la stratégie de sécurité de l'information, afin de faire des ressources humaine le maillon fort de la chaine de sécurité*

Règles

1) Une charte d'utilisation des ressources informatiques est élaborée par le RSSI et validée et diffusée par le CSI. Cette charte d'utilisation énonce les conditions et règles d'utilisation appropriées des ressources informatiques mises à disposition des usagers.
2) Elle définit de manière claire et non ambiguë les règles, actions proscrites et les mesures disciplinaires applicables dans le cadre de l'usage des ressources informatiques, accès au système d'information, etc.
3) La charte d'utilisation est signée par tous les agents et contresignée par le Responsable de la Sécurité des Systèmes d'Information et le responsable des ressources humaines.
4) Une clause de confidentialité et de non-divulgation est ajoutée dans les contrats des personnels assurant des fonctions clés en matière de sécurité de l'information ou toute autre fonction donnant accès à des informations sensibles au sein de l'entité. Elle définit les conditions générales et spécifiques relative à la confidentialité et la non-divulgation des informations auxquelles l'employé ou l'agent a accès durant ou après ses fonctions au sein de l'entité.

5) GESTION DES ACTIFS INFORMATIONNELS

Inventaire et propriété des actifs

Objectifs :

- *Identifier ses actifs informationnels,*
- *cartographier son système d'information*
- *définir les responsabilités appropriées en matière de protection.*

Règles

1) Chaque entité doit réaliser et maintenir à jour un inventaire de ses ressources informatiques. Cet inventaire comprend la liste des matériels et logiciels, leurs versions exactes, ainsi que les fichiers de configuration des maintenus et mis à jour ;
2) Pour chaque actif inventorié, un propriétaire est nommément désigné et informé. Il est responsable de l'actif et prend toutes les mesures utiles tout au long du cycle de vie de l'actif ;
3) Cet inventaire est conservé dans les conditions de sécurité suffisantes et conformes à la législation en vigueur, notamment le Référentiel Général de Sécurité des Systèmes d'Information (RGSI). Il est tenu à disposition du RSSI et de l'ARTCI pour les besoins de coordination opérationnelle en cas de gestion de crise.
4) La cartographie du système d'information indique les vues, les zones et l'organisation structurelle du système d'information. Cette cartographie est maintenue et tenue à la disposition du RSSI et de l'ARTCI, pour les besoins de coordination opérationnelle en cas de gestion de crise.

Classification des actifs

Objectifs

- *Définir un niveau de protection approprié en fonction de l'importance de l'actif*

Règles

1) L'entité définit des critères de classification de l'information en fonction de la sensibilité de l'information, des besoins de partage et son importance. Les critères de classification et les modalités de traitement sont définis par le RSSI et validés par le CSI.
2) Tous les biens sont classifiés et formellement documentés.
3) Une procédure de marquage systématique de l'information est élaborée et communiquée. Le responsable de l'actif est responsable de sa classification et de la mise en œuvre des mesures adéquates pour son traitement conformément aux critères de classification définis. Le système de marquage est élaboré de sorte à faciliter la reconnaissance des indications et besoins de sécurité correspondants.

6) CONTRÔLE D'ACCES

Objectifs

- *Définir les conditions d'accès aux ressources des SI de l'Etat*
- *Maitriser les accès aux ressources des SI de l'Etat*

Règles

1) Chaque entité doit élaborer et mettre en œuvre une politique de contrôle d'accès qui couvre les règles relatives au contrôle d'accès logique et physique aux ressources de son SI,
2) L'accès aux ressources non publiques du SI est accordé exclusivement aux usagers enregistrés sous un identifiant unique qui permet de relier l'utilisateur à ses actions et de les lui imputer.
3) Un registre centralisé de tous les droits d'accès accordés aux utilisateurs enregistrés est élaboré et tenu à jour sous la supervision du responsable de sécurité de l'information (RSSI).
4) L'attribution des privilèges d'accès fait l'objet d'une procédure documentée et communiquée au sein de l'entité. Chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde l'autorisation d'accès ;
5) Les droits d'accès sont revus périodiquement par le RSSI, afin de tenir compte des changements, évolutions et modification du contexte organisationnel de l'entité. Ils sont soit supprimés, soit adaptés aux besoins de l'entité ;
6) Les mots de passe, clés secrètes, etc., permettant d'accéder aux ressources du système d'information de l'Etat sont des informations sensibles et doivent être traitées comme tel par les utilisateurs, conformément à la politique de classification de l'information adoptée par l'entité.
7) L'entité élabore et met en œuvre une politique de gestion des mots de passe.
8) Chaque compte utilisateur est créé avec un mot de passe initial généré aléatoirement. L'utilisateur doit modifier son mot de passe après la première utilisation.
9) L'entité met en œuvre des moyens techniques, afin d'imposer des exigences de qualité et de robustesse des mots de passe lorsque ceux-ci sont créés par les utilisateurs eux-mêmes.
10) Les mots de passe ou moyens d'authentification donnant un accès pour l'administration des ressources de l'Etat, font l'objet de dispositions spéciales. Le niveau d'exigence pour les mots de passe des administrateurs de systèmes d'information de l'Etat est très élevé. A cet effet, des règles spéciales de protection de la confidentialité leurs sont appliquées et les exigences communiquées à leurs propriétaires.
11) Le RSSI doit documenter toutes les autorisations accordées et les programmes utilitaires à privilèges installés sur les ressources du système d'information.
12) Une procédure documentée est élaborée et mise en œuvre pour l'habilitation des administrateurs. Cette procédure définit les modalités d'accès aux espaces d'administration et les règles de sécurité y attachées.
13) Le nombre et l'identité des administrateurs habilités sont approuvés par le CSI sur proposition du RSSI.

7) USAGE DE LA CRYPTOGRAPHIE

Objectifs

- *Protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.*
- *Être conforme avec les exigences légales en la matière et les bonnes pratiques de l'industrie*

Règles

1) Lorsqu'elle fait usage de moyens cryptographiques, l'entité est tenue d'élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.
2) Cette politique définit les orientations stratégiques, ainsi que les rôles et responsabilités pour la gestion technique des moyens cryptographiques et les normes techniques adoptées.
3) La politique est alignée sur les exigences légales et réglementaires définies par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire qui assume les fonctions d'Autorité Nationale de Certification.

8) SECURITE PHYSIQUE ET ENVIRONNEMENTALE

Zones sécurisées

Objectifs

- *Découper le site en zones de niveau de sensibilité*
- *Protéger l'accès physique aux zones contenant des ressources informatiques sensibles*

Règles

1) Les sites abritant les ressources des systèmes d'information de l'Etat sont découpés en zones. Pour chaque zone, les moyens de protection et les critères d'accès physique sont définis en tenant compte de la sensibilité des informations et des installations qui y sont stockées. Cette tâche est réalisée par le RSSI avec la collaboration des départements chargés des moyens généraux, de l'immobilier, de la sécurité, etc.
2) L'entité doit mettre en œuvre des moyens d'identification et de catégorisation des personnes accédant à ses locaux (agents, visiteurs, prestataires, fournisseur, etc.)
3) Les restrictions d'accès à certaines zones doivent être clairement notifiées aux visiteurs et agents, en fonction des critères de sensibilité retenus pour les zones sécurisées.
4) L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

Protection des matériels et supports papier

Objectifs

- *Assurer la protection et la disponibilité des équipements sensibles*
- *Réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé*

Règles

1) Les moyens de traitement de l'information manipulant des données sensibles, sont positionnés avec soin, en vue de réduire le risque que cette information puisse être vue par des personnes non autorisées.
2) L'entité prend et met en œuvre des mesures techniques pour protéger les installations sensibles contre les ruptures d'alimentation électriques, la foudre, les incendies, etc.
3) Le RSSI doit établir et mettre en œuvre une procédure documentée relative à la sortie du matériel ou d'actifs.
4) Le RSSI doit formaliser et mettre en œuvre une procédure de mise au rebut et de restitution des actifs.

9) SECURITE LIEE A L'EXPLOITATION

Procédures et responsabilités liées à d'exploitation

Objectifs

- *s'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.*
- *contrôler les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information.*

Règles

1) Chaque entité établit des procédures documentées et approuvées par le CSI, pour les activités d'exploitation liées aux moyens de traitement de l'information et de la communication. Ces procédures couvrent notamment les aspects liés à :
    a. l'installation et la configuration des systèmes ;
    b. le traitement et la manipulation de l'information, qu'ils soient automatisés ou manuels ;
    c. la sauvegarde des données ;
    d. les exigences de planification, y compris les interdépendances avec d'autres systèmes, et les heures de démarrage de la première tâche et d'achèvement de la dernière tâche ;
    e. la procédure de redémarrage et de récupération du système à appliquer en cas de défaillance du système ;

f. la gestion du système de traçabilité et de l'information des journaux système ;

g. la surveillance des procédures.

2) Pour chaque procédure, les rôles et responsabilités des acteurs sont clairement définis.

3) Tous les changements au sein de l'organisation ayant un impact sur la sécurité de l'information doivent être contrôlés et effectués avec le concours du RSSI. Ce dernier prend toutes les mesures nécessaires pour s'assurer que la mise en œuvre de ces changements ne désorganise pas la sécurité ou alors il s'assure que les modifications nécessaires sont apportées à la sécurité pour intégrer harmonieusement les changements.

Protection contre les logiciels malveillants

Objectifs

- *Protéger les logiciels et l'information contre les codes malveillants*

Règles

1) Des logiciels antivirus sont installés et configurés uniformément sur tous les serveurs et postes de travail de l'entité. Pour chaque catégorie une configuration spécifique est adoptée en fonction des besoins de sécurité y attachés.

2) Les mises à jour des logiciels antivirus sont effectuées régulièrement.

3) Des mesures sont mises en œuvre pour sensibiliser et former les utilisateurs sur les règles de bon usage des logiciels antivirus.

4) Des mesures techniques sont mises en œuvre pour empêcher l'accès depuis les ressources du système d'information de l'entité à certains sites ou applications réputés pour leur malveillance ou pour leur dangerosité.

5) Une veille technique de sécurité sur les vulnérabilités techniques des logiciels et systèmes d'exploitation utilisés au sein de l'entité est effectuée comme tâche régulière, selon une périodicité et une procédure définie par le RSSI.

6) Une procédure spéciale pour assurer la continuité et/ou la reprise des activités en cas d'attaque par un logiciel malveillant est définie et régulièrement testée.

Sauvegarde

Objectifs

- *Maintenir l'intégrité et la disponibilité des informations et assurer leur restauration*

Règles

1) Le RSSI doit s'assurer de la définition et la mise en œuvre de la politique de sauvegarde. Elle définit :
    a. Les responsables de la sauvegarde
    b. La fréquence
    c. Le type
    d. Le support
    e. La durée et les conditions de conservation des copies
    f. Les modalités de mises en œuvre du test de restauration

Journalisation et surveillance

Objectifs

- *Enregistrer les événements et générer des preuves*

Règles

1) La création et l'enregistrement systématique des journaux d'événements sur les postes de travail, serveurs et autres matériels est obligatoire, afin d'assurer la traçabilité et l'imputabilité des activités effectuées sur le système d'information.
2) Les journaux d'événement ou logs sont susceptibles de contenir des données sensibles ou des données à caractère personnel. A ce titre, toutes les mesures sont mises en œuvre pour les protéger de tout accès non autorisé.
3) Les journaux d'événement peuvent être utilisés comme éléments de preuve à charge ou à décharge dans le cadre d'une instruction judiciaire ou une procédure administrative. A ce titre, ils doivent être protégés de sorte qu'aucune modification, altération ou suppression indue ne soit réalisée.
4) Les mesures techniques de configuration de la précision et synchronisation des horloges doivent être mises en œuvre, afin d'horodater avec exactitude les activités enregistrées dans les journaux d'événements.

Installation de logiciels sur des systèmes en exploitation

Objectifs

- *contrôler les logiciels qui sont installés sur les systèmes en exploitation*
- *prévenir les risques de perturbation du fonctionnement des systèmes en exploitation*

Règle

1) L'installation de logiciels sur des systèmes en exploitation est réalisée exclusivement par un administrateur habilité et qualifié.
2) Une procédure relative à l'installation des logiciels sur des systèmes en production est élaborée et mise en mise en œuvre. Elle définit les exigences en matière de :
    a. Test de compatibilité avec le système
    b. Etude des failles et vulnérabilités connues
    c. Mises à jour des versions
3) L'ensemble des logiciels installés est documenté, consigné dans le registre d'inventaire des actifs.

Gestion des vulnérabilités

Objectifs

- *Détecter les vulnérabilités techniques*
- *Empêcher l'exploitation des vulnérabilités techniques*

Règles

1) L'entité définit et met en œuvre une procédure de gestion des vulnérabilités technique. Celle-ci définit :
    a. Les rôles et responsabilités ;
    b. Les mécanismes de collecte d'informations relatives aux vulnérabilités techniques ;
    c. Le flux de travail à partir du moment où l'information est collectée, jusqu'aux mesures opérationnelles à mettre en œuvre pour corriger les vulnérabilités techniques ;

10) SECURITE DES COMMUNICATIONS

Gestion de la sécurité des réseaux

Objectifs

- *Protéger l'information sur les réseaux et les moyens de traitement de l'information sur lesquels elle s'appuie.*

Règles

1) La gestion des équipements réseau est du ressort des équipes informatiques habilitées au sein de l'entité. Seuls les équipements autorisés par les équipes informatiques de l'entité ont le droit de se connecter au réseau local.
2) Les systèmes connectés sur le réseau doivent être authentifiés et leurs activités journalisées.
3) Les réseaux sont nécessairement divisés en domaines séparés, établis en fonction des niveaux de sécurisation, notamment : **domaine d'accès public, domaine postes de travail, domaine serveurs**. Le périmètre de chaque domaine est défini en fonction des exigences et du contexte de l'entité.
4) L'accès entre les différents domaines du réseau est autorisé, mais nécessairement contrôlé au niveau de chaque périmètre par une passerelle (pare-feu, routeur-filtre, etc.).
5) Les accès sans-fil sont considérés comme des connexions externes et doivent être séparés des accès des réseaux internes jusqu'à franchissement de la passerelle (pare-feu, routeur filtre) avant d'accéder aux systèmes internes.

Transfert de l'information

Objectifs

- *Protéger les flux d'information échangés via des canaux de communication électronique avec l'extérieur*

Règles

1) En tenant compte de la politique de classification de l'information, des moyens techniques de chiffrement de l'information doivent être utilisés pour des informations d'un certain niveau de sensibilité.
2) L'information sensible doit être chiffrée sur les supports amovibles, avant leur transfert vers l'extérieur
3) Des accords de transfert de l'information doivent être établis avec les tiers, afin de tenir des exigences définies par la politique de classification de l'information et les exigences de sécurité et de protection qui y sont attachées.

11) ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION.

Objectifs

- *Intégrer la sécurité de l'information dans le cycle de vie de tous les systèmes d'information*
- *Réduire les risques liés à l'exploitation des vulnérabilités techniques*

Règles

1) Les développements et les acquisitions doivent prendre en compte les besoins des métiers en matière de sécurité de l'information. Une analyse des besoins de sécurité doit nécessairement être effectuée, afin de prendre en compte les exigences de sécurité associées.
2) L'aspect sécurité de l'information doit être intégré à tous les projets dès la phase de conception. A cet effet, le RSSI ou un analyste de sécurité des SI (ASSI) doit obligatoirement être intégré dans tous les projets initiés par l'entité, afin d'intégrer les exigences en matière de sécurité de l'information dès la conception du projet.
3) Un guide d'exigences relatif au développement d'applications est élaboré sous la responsabilité du RSSI. Il s'applique à tous les projets de développement au sein de l'entité.
4) Pour les développements externalisés, des clauses de sécurité des systèmes d'information doivent être inclues dans les contrats de sous-traitance. Ils couvrent les rubriques suivantes :
    a. Formation obligatoire des développeurs sur le développement sécurisé et les vulnérabilités classiques
    b. Utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils d'analyse statique de code, bibliothèques sécurisées, etc.)
    c. Production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.)
    d. Respect de normes de développement sécurisé
    e. Obligation pour le prestataire de corriger dans un temps raisonnable, les vulnérabilités introduites durant le développement
5) Des audits de vulnérabilités des applications, bases de données et systèmes sensibles sont réalisés à intervalle régulier, notamment en cas de changement apportés à la plateforme d'exploitation, d'apparition d'une vulnérabilité majeure.

12) RELATIONS AVEC LES FOURNISSEURS

Sécurité de l'information dans les relations avec les fournisseurs

Objectifs

- *S'assurer que les fournisseurs et autres prestataires de services respectent les exigences de sécurité appliquées aux systèmes d'information*

Règle

1) Chaque entité élabore des clauses relatives à des mesures de sécurité spécifiques aux accès des fournisseurs à l'information de l'organisation, dans les contrats de services. Les mesures incluent dans les contrats de service sont cohérentes avec les processus et procédures de sécurité mis en œuvre par l'entité.
2) L'entité doit imposer également des mesures et procédures de sécurité que le fournisseur doit mettre en œuvre pour les communications, le traitement de l'information auquel il a accès.

13) GESTION DES INCIDENTS

Gestion des incidents liés à la sécurité de l'information et améliorations

Objectifs

- *Communiquer les alertes relatives aux événements et failles liés à la sécurité de l'information*
- *Mettre en place une stratégie globale cohérente et efficace pour la prise en charge des alertes*
- *Traiter les incidents, afin de restaurer la sécurité en cas d'incidents et assurer la continuité des activités*

Règles

1) Le RSSI et les acteurs opérationnels (ASSI) mettent en œuvre chacun à leur niveau, les mesures nécessaires pour faciliter la coordination du traitement d'incidents en cas de graves crises.
2) Toutes les entités doivent définir une procédure de gestion des incidents de sécurité informatique qui précise les rôles et responsables des acteurs clés et le flux de travail pour le traitement d'un incident.
3) La procédure implique nécessairement les mécanismes et responsabilités pour la remontée de l'information au CI-CERT.
4) Une procédure de réponse d'urgence en cas d'infection par un logiciel malveillant ou tout autre code malveillant est défini et communiquée à tous les utilisateurs. Elle définit également l'obligation de signaler sans délais tout cas d'infection ou d'événement de sécurité et les moyens de le faire.
5) L'ensemble des incidents de sécurité enregistrés sont consignés dans un document et tenu à la disposition de l'ARTCI pour les besoins de coordination opérationnelle.

14) ASPECTS DE LA SECURITE DE L'INFORMATION DANS LA GESTION DE LA CONTINUITE DE L'ACTIVITE

Plan de continuité d'activités

Objectifs

- *Elaborer un plan de continuité des activités*
- *Intégrer la continuité des activités dans la gestion de la sécurité de l'information*

Règles

1) Chaque entité élabore un programme de récupération après sinistre qui identifie les services et matériels essentiels pour le fonctionnement continu des activités. Des mesures techniques pour assurer suffisamment la redondance de ces actifs essentiels pour le fonctionnement continu de l'entité sont définies et régulièrement testées.
2) Les exigences de sécurité de l'information restent les mêmes dans des situations défavorables que dans des conditions d'exploitation normales. A ce titre, les règles de sécurité et politiques applicables restent les mêmes en situation de fonctionnement normal ou en cas de sinistre ou de graves crises.
3) Pour les cas extrêmes, les changements ou modification des règles de sécurité doivent être expressément autorisées par le RSSI, après approbation du CSI.

15) CONFORMITE

Objectifs

- *S'assurer de la conformité de la sécurité du système d'information par rapport aux exigences légales et réglementaires en vigueur en matière de sécurité de l'information.*

Règles

1) Le respect de la conformité à la PSSI est une exigence réglementaire. Le RSSI s'assure de la conformité de la politique de sécurité des systèmes d'information de l'entité avec la PSSI, à travers de contrôles réguliers.
2) Chaque entité doit soumettre son système d'information à l'audit de sécurité réalisé par l'ARTCI et selon les règles et dispositions réglementaires en vigueur.
3) Les exigences en matière de respect des droits de propriété intellectuelle, protection des données à caractère personnel, cryptographie et toutes autres réglementations en vigueur sont identifiées et des mesures adéquates sont mises en œuvre.
4) Chaque entité désigne un correspondant à la protection des données à caractère personnel conformément aux dispositions légales.

GLOSSAIRE

ARTCI : Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire

ASSI : Analyste de sécurité des systèmes d'information

CERT : Computer Emergency Response Team

CI-CERT : Côte d'Ivoire – Computer Emergency Response Team

CSI : Comité Sécurité de l'Information

DAF : Direction des Affaires Administratives et Financières

DAJ : Direction des Affaires Juridiques

DITT : Direction de l'Informatique t des Traces technologiques

DRH : Direction des ressources humaines

DSI : Direction des Systèmes d'Information

PLCC : Plateforme de Lutte Contre la Cybercriminalité

PSSI : Politique Nationale de Sécurité des systèmes d'information

RGSSI : Référentiel Général de Sécurité des Systèmes d'Information

SI : Systèmes d'information

SSI : Sécurité des Systèmes d'Information

Incident de sécurité des systèmes d'information ou incident de sécurité ou incidents : événement affectant la sécurité des systèmes informatique, notamment dans sa disponibilité, intégrité, confidentialité. Sont exclus des champs des incidents, dans le cadre de cette politique : les pertes de matériel, les atteintes à l'intégrité physiques des personnes.

Entité : organe administratif ou technique fournissant des services pour le compte de l'Etat, notamment les ministères, institutions d'Etat, Autorités administratives, établissements publics et entités sous-tutelles (agences, centres nationaux, bureaux d'études, etc.), collectivités territoriales.

ANNEXES

[Nom de l'entité]

[Titre de la politique]

Référence	*Nomenclature adoptée par l'entité pour référencer les documents*
Version	*Dernière version du document*
Date de la version	*Date de dernière révision/modification du document*
Statut	*Statut actuel du document (validé, publié, en attente de validation, draft)*
Créé par	*Auteur(s) du document*
Approuvé par	*Nom, Prénoms et fonction de la personne qui valide le document*
Propriétaire	*Nom, Prénoms et fonction du propriétaire du document*
Niveau de confidentialité	*Classification de la sensibilité du document*
Diffusion	Règles de diffusion applicables (restreinte, publique, interdite)

HISTORIQUE DES MODIFICATIONS			
Date	*version*	*Créé par*	*Description de la modification*
JJ-MM-AAAA	*1.0*	*ARTCI*	*Structure documentaire de base*

1) BUT, DOMAINE D'APPLICATION

***But** : pourquoi ce document est-il élaboré ?*

***Domaine d'application** : Quelles sont les actifs (matériels, logiciels) qui sont couverts par ce document ?*

2) AUDIENCE

A qui ce document s'adresse-t-il ? Quelles sont les personnes qui sont concernées par les règles de sécurité contenues dans ce document ?

3) REFERENCES DOCUMENTAIRES

Quels sont les documents et les exigences cadres à partir desquels les règles contenues dans ces documents sont élaborées ?

4) ENNONCE DES REGLES DE SECURITE

Lister points par points les règles de sécurité et les détails de mise en œuvre de ces règles de sécurité

5) VALIDITE ET GESTION DOCUMENTAIRE

Ce document est valide dès le [date]

Le propriétaire de ce document, M. / Mme / Mlle [Nom, Prénoms et fonctions du propriétaire], est chargé de vérifier et si nécessaire mettre à jour le document au moins une fois par an.

Pour évaluer l'efficacité et l'adéquation de ce document, les critères suivants doivent être considérés :

Lister des critères d'évaluation par rapport à l'objet du document

[Titre du poste]

[Nom, Prénoms]

_____

[Signature]

LETTRE D'ENGAGEMENT POUR LA PROTECTION DE L'INFORMATION

Chers collaborateurs,

La protection des informations et la sécurité du système d'information de [*nom de l'organisation*] contribuent grandement à la bonne exécution des missions qui nous sont dévolues et la préservation d'un climat de confiance et de stabilité de l'Etat tout entier. A l'heure du numérique, nous sommes résolument tournés vers une digitalisation de notre société, afin de profiter des énormes potentialités offertes par les technologies de l'information et de la communication. Cependant, notre organisation comme toutes les autres à travers le monde, doit faire face à des risques de sécurité liés à la protection des données des citoyens, des agents et fonctionnaires de l'Etat, etc., contre les attaques malveillantes ou erreurs accidentes susceptibles de mettre à mal le bon fonctionnement la confiance des usagers et la stabilité socio-économique du pays.

A ce titre, il est vital de protéger les informations que nous stockons, partageons quotidiennement dans le cadre de l'accomplissement de nos missions, par le biais des systèmes d'information. En effet, chaque utilisateur du système d'information doit être conscient que son rôle est capital pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité des données traitées. Garantir la sécurité de l'information est une responsabilité partagée et un gage de confiance sur la qualité, l'efficacité et la disponibilité du service public offert à nos concitoyens.

Nous avons mis en place une organisation spécifique au sein de notre entité, afin de piloter et coordonner la sécurité de l'information. A cet effet, un Responsable de la Sécurité de l'Information (RSSI) est désigné, en conformité avec les exigences réglementaires, afin de coordonner et mettre en cohérence les besoins de sécurité de l'information et les exigences métiers, dans l'intérêt supérieur de la satisfaction des usagers du service public.

J'invite tous les collaborateurs à participer pleinement à la mise en œuvre de la stratégie de protection de l'information définie par le RSSI et les services compétents, à travers le respect des règles et politiques de sécurité définies.

Je me félicite d'avance de notre engagement responsable à œuvrer tous ensemble, pour l'atteinte des objectifs fixés.

Fait à Abidjan, le 22 décembre 2021

Copie certifiée conforme à l'original
Le Secrétaire Général du Gouvernement

Alassane OUATTARA

RÉPUBLIQUE DE CÔTE D'IVOIRE
SECRÉTARIAT GÉNÉRAL DU GOUVERNEMENT

Eliane Atté BIMANAGBO
Préfet

Nº 2101066