67e Année N° 31 ter

NUMERO SPECIAL

12 Août 2022

JOURNAL OFFICIEL

DE LA REPUBLIQUE TOGOLAISE

PARAISSANT LE 1er ET LE 16 DE CHAQUE MOIS A LOME

TARIF

ACHAT	ABONNEMENT ANNUEL	ANNONCES
• 1 à 12 pages..... 200 F • 16 à 28 pages ..... 600 F • 32 à 44 pages ..... 1000 F • 48 à 60 pages ..... 1500 F • Plus de 60 pages ..... 2 000 F	• TOGO..... 20 000 F • AFRIQUE..... 28 000 F • HORS AFRIQUE ..... 40 000 F	• Récépissé de déclaration d'associations .. 10 000F • Avis de perte de titre foncier (1er et 2e insertions) ..... 20 000 F • Avis d'immatriculation ..... 10 000 F • Certification du JO ..... 500 F

NB. : Le paiement à l'avance est la seule garantie pour être bien servi.
Pour tout renseignement complémentaire, s'adresser à l'EDITOGO Tél. : (228) 22 21 37 18 / 22 21 61 07 / 08 Fax (228) 22 22 14 89 - BP: 891 - LOME

DIRECTION, REDACTION ET ADMINISTRATION

CABINET DU PRESIDENT DE LA REPUBLIQUE - TEL. : 22 21 27 01 - LOME

SOMMAIRE

PARTIE OFFICIELLE

ACTES DU GOUVERNEMENT DE LA REPUBLIQUE TOGOLAISE

LOIS, ORDONNANCES, DECRETS, ARRETES ET DECISIONS

ARRETES

PARTIE OFFICIELLE

ACTES DU GOUVERNEMENT DE LA REPUBLIQUE TOGOLAISE

LOIS, ORDONNANCES, DECRETS, ARRETES ET DECISIONS

ARRETES

ARRETE N° 2022-040/PMRT DU 29/06/2022 portant adoption des règles de cybersécurité en République togolaise

LE PREMIER MINISTRE,

Vu la Constitution du 14 octobre 1992 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité (ANCy) ;

Vu le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du Gouvernement, complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu le décret n° 2021-045/PR du 29 avril 2021 portant nomination du directeur général de l'Agence nationale de la cybersécurité ;

ARRETE :

Article premier : Objet

Le présent arrêté porte adoption des règles de cybersécurité applicables aux opérateurs de services essentiels désignés par l'Agence nationale de la cybersécurité, et à toute l'administration publique togolaise.

Les règles de cybersécurité annexées au présent arrêté en font partie intégrante.

Art. 2 : Application

Les ministres et les premiers responsables des institutions de la République veillent, chacun en ce qui le concerne, à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels relevant de leur ressort.

Art. 3 : Exécution

Le directeur général de l'Agence nationale de la cybersécurité (ANCy) est chargé de l'exécution du présent arrêté qui sera publié au Journal Officiel de la République Togolaise.

Fait à Lomé, le 29 juin 2022

Le Premier ministre

Victoire S. TOMEGAH-DOGBE

ANNEXE

REGLES DE CYBERSECURITE EN REPUBLIQUE TOGOLAISE

MINISTERE DE L'ECONOMIE
NUMERIQUE ET DE LA
TRANSFORMATION DIGITALE

MINISTERE DE LA SECURITE
ET DE LA PROTECTION CIVILE

ANCy
Agence Nationale
de la Cybersécurité

Règles de Cybersécurité

Version 1.0

Juin 2022

Table des matières

1. Cadre légal et réglementaire

Les présentes Règles de Cybersécurité sont établies dans le cadre de la législation togolaise, en particulier des textes législatifs et règlementaires suivants :

- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (« **Loi sur les Données Personnelles** ») ;
- La loi n°2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité (« **Loi sur la Cybersécurité** ») ;
- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise (« **Loi sur les Transactions Electroniques** ») ;
- La loi d'orientation n°2017-006 du 22 juin 2017 sur la société de l'information au Togo (« **Loi sur la Société de l'Information** ») ;
- La loi n°2014-014 du 22 octobre 2014 portant modernisation de l'action publique de l'Etat en faveur de l'économie (« **Loi sur la Modernisation de l'Action Publique** ») ;
- La loi no 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n°2013-003 du 19 février 2013 (« **Loi sur les Communications Electroniques** ») ;
- Le décret n°2021-102/PR du 29 septembre 2021 portant création, attributions, organisation et fonctionnement de l'Agence Togo Digital (ATD) ;
- Le décret n°2021-031/PR du 24 mars 2021 portant numérisation des paiements de l'Administration publique ;
- Le décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo (« **Décret sur les Transactions Electroniques** ») ;
- Le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) (« **Décret CDA** »).
- Le décret n°2019-095/PR du 8 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes (« **Décret OSE** ») ;
- Le décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité (ANCy) (« **Décret ANCy** ») ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national (« **Arrêté PSCE** »).

2. Définitions

En plus des termes définis dans la loi sur la Cybersécurité, dans le préambule, l'introduction et/ou dans les autres paragraphes de ce document, les acronymes et termes suivants sont définis comme suit :

Délégataire de l'ANCy : La société d'économie mixte Cyber Defense Africa S.A.S. (CDA), ayant son siège social à Lomé et ayant signé avec l'ANCy un contrat de délégation de service public portant sur la création et l'exploitation de structures permettant de sécuriser le cyberespace togolais et chargeant CDA de fournir des solutions nécessaires (infrastructure informatique, logiciels et services) afin de prévenir, analyser et répondre aux attaques informatiques et cyberattaques visant ou impliquant des systèmes informatiques ou systèmes d'information appartenant à des opérateurs de services essentiels et/ou autres organisations installées sur le territoire de la République togolaise.

La liste à jour des délégataires de l'ANCy peut être trouvée sur le site Internet de l'Agence.

CERT National : Equipe nationale de gestion des incidents de cybersécurité fournissant des services de CERT (*Computer Emergency Response Team*) National sur le territoire de la République togolaise.

Personnel Essentiel : Personnel de l'OSE (interne ou externe, qu'il soit lié par un contrat de travail, de service ou toute autre relation contractuelle) nécessaire à la fourniture continue et ininterrompue du ou des Service(s) Essentiel(s) de l'OSE.

Prestataire de services de confiance en cybersécurité qualifié par l'ANCy : prestataires fournissant des services qui contribuent à la sécurité (i) des systèmes d'information des administrations ou des opérateurs de services essentiels et (ii) de tout matériel, logiciel ou système d'information destiné à traiter des informations couvertes par le secret de la défense nationale.

SOC : désigne un Security Operation Center ou Centre opérationnel de sécurité ;

3. Introduction

Conformément au Décret ANCy, l'Agence Nationale de la Cybersécurité (ANCy) est l'autorité nationale en matière de sécurité des systèmes d'information au Togo. Elle concourt à la définition et à la mise en œuvre de la politique et des orientations stratégiques du pays en matière de cybersécurité.

Le Décret OSE définit les modalités et critères de désignation des opérateurs de services essentiels (ci-après les « **Opérateurs de Services Essentiels** » ou « **OSE** »), de déclaration des infrastructures essentielles situées sur le territoire togolais (les « **Infrastructures Essentielles** » ou « **IE** ») et fixe les obligations et règles relatives à la cybersécurité desdites Infrastructures Essentielles. Les services essentiels des OSE (ci-après les « **Services Essentiels** ») sont listés en annexe du Décret OSE.

Les présentes Règles de Cybersécurité sont fixées par l'ANCy conformément à l'article 11 du Décret OSE et s'articulent autour des quatre domaines suivants :

1. **La gouvernance de la sécurité des réseaux et systèmes d'information**
2. **La protection des réseaux et systèmes d'information**
3. **La défense des réseaux et systèmes d'information**
4. **La résilience des activités**

Pour chaque domaine, ces règles définissent les contrôles appropriés dans chacun des sous-domaines suivants :

1. **La gouvernance de la sécurité des réseaux et systèmes d'information (G)**
   - G1. Gouvernance, Gestion et Leadership
   - G2 - Politique de sécurité et Plan de Sécurité d'Opérateur (PSO)
   - G3. Conformité, audit et performance
   - G4. Gestion des risques de cybersécurité
   - G5. Ressources humaines
   - G6. Relations avec les fournisseurs
2. **La protection des réseaux et systèmes d'information (P)**
   - P1. Contrôle d'accès
   - P2. Gestion des actifs
   - P3. Sécurité des réseaux et des communications
   - P4. Systèmes d'information, acquisition et maintenance
   - P5. Sécurité des opérations
   - P6. Sécurité environnementale et physique
3. **La défense des réseaux et systèmes d'information (D)**
   - D1. Gestion des incidents de sécurité
4. **La résilience des activités (R)**
   - R1. Gestion de la continuité des activités

Le tableau ci-dessous décrit chacun des sous-domaines mentionnés ci-dessus

Réf.	Domaine de contrôle	Description
G1	Gouvernance, gestion et leadership	Préparer le terrain pour la mise en place efficace de la fonction de cybersécurité au sein de l'OSE, en identifiant les principaux intervenants, leurs rôles et responsabilités connexes.
G2	Politique de sécurité et plan de sécurité d'opérateur (PSO)	Fournit un ensemble de directives de politique de cybersécurité que les OSE peuvent adopter et mettre en œuvre.
G3	Conformité, Audit et performance	Fournit des contrôles pour garantir la conformité aux règles, aux performances et à la surveillance requises.
G4	Gestion des risques de cybersécurité	Traite des contrôles et des pratiques d'identification et de gestion des risques.
G5	Ressources humaines	Répertorie les contrôles, les exigences et vérifications à effectuer pour fournir une assurance et une minimisation des risques liés aux comportements et aux personnes.
G6	Relations avec les fournisseurs	Fournit des pratiques sécurisées à inclure dans l'engagement de fournisseurs et de tiers, y compris le traitement des données, le flux d'informations, etc..
P1	Contrôle d'accès	Détaille les contrôles à mettre en œuvre pour un accès sécurisé à l'infrastructure numérique des OSE, y compris, mais sans s'y limiter, aux locaux, aux systèmes d'exploitation, etc.
P2	Gestion des actifs	Détaille les contrôles à appliquer pour la gestion des actifs informationnels critiques.
P3	Sécurité des réseaux et des communications	Fournit des exigences et des contrôles pour la mise en œuvre, l'utilisation et l'exploitation sécurisées des systèmes, des télécommunications, de la messagerie et des réseaux des OSE pour le transfert, le traitement et le stockage de données sensibles.
P4	Systèmes d'information, acquisition et maintenance	Répond aux exigences en matière des acquisitions, de développement et de gestion des systèmes d'information sécurisés.
P5	Sécurité des opérations	Fournit des contrôles pour effectuer des opérations sécurisées des OSE.
P6	Sécurité environnementale et physique	Identifie l'ensemble des contrôles nécessaires à mettre en place ou à améliorer en matière de sécurité physique lors de l'accès aux installations des OSE.
D1	Gestion des incidents de sécurité	Fournit des conseils et des contrôles en vue de l'identification précoce des menaces potentielles à la sécurité et de la prise de mesures d'atténuation immédiates.
R1	Gestion de la continuité des activités	Assure la résilience et la continuité des opérations face aux événements désastreux imprévus pour les OSE.

Conformément au Décret OSE, les Opérateurs de Services Essentiels doivent respecter les présentes Règles de Cybersécurité, sous peine de sanctions.

Les présentes Règles de Cybersécurité peuvent être modifiées en cas de besoin et ce au moins tous les deux (2) ans.

4. Contrôle de conformité de la sécurité des Infrastructures Essentielles (IE) et accréditation

La société CDA est chargée du contrôle annuel des OSE par un contrat de délégation de service signé avec l'ANCy. Ce contrôle vise à vérifier l'application et l'efficacité des mesures de sécurité du PSO pour chaque IE dans le respect des présentes Règles de Cybersécurité.

A l'issue de l'audit de conformité, la société CDA élabore un rapport d'audit qui expose les constatations sur les mesures appliquées et sur le respect du PSO et des présentes Règles de Cybersécurité. Le rapport précise si le niveau de sécurité atteint est conforme aux objectifs de sécurité du PSO, compte tenu des menaces et des vulnérabilités connues. Il formule des recommandations pour remédier aux éventuelles non-conformités et vulnérabilités découvertes. Le rapport est couvert par le secret professionnel, comme toute l'activité du délégataire de l'ANCy.

Lors de cette procédure d'accréditation, prenant en compte les évènements intervenus durant l'année écoulée, le PSO de l'OSE est mis à jour avec notamment une éventuelle redéfinition des objectifs, de la stratégie et des mesures mises en place.

5. Domaines et sous-domaines des règles de cybersécurité

Dans cette section, des domaines et sous-domaines ont été identifiés comme mesures de contrôles qui fournissent des exigences de sécurité pour un niveau minimum de protection contre la cybercriminalité croissante pour les actifs informationnels et les systèmes sous-jacents de tous les OSE.

L'adoption accrue de la numérisation, des communications électroniques et du cyberespace, composé d'un réseau mondial d'infrastructures de réseau interdépendantes, de réseaux de télécommunications et de systèmes de traitement informatique, a entraîné des progrès dans les services numériques ainsi que des cybermenaces.

Au fur et à mesure que les cybermenaces telles que l'hacktivisme et la cybercriminalité évoluent, les efforts visant à les combattre de manière coordonnée et systématique doivent également évoluer. Pour aligner et diriger les efforts nationaux de cybersécurité, L'ANCy a développé un ensemble de règles de cybersécurité à respecter par tous les OSE.

Ces règles sont classées en quatorze sous-domaines avec les principaux contrôles et sous-contrôles qui doivent être mis en œuvre par les OSE.

La conformité à ces règles fournira une base de protection minimale pour les OSE et accordera des capacités pour dissuader les cyberattaques de manière cohérente dans tout le pays ainsi que pour promouvoir un environnement numérique de confiance pour les particuliers et les entreprises.

Plus précisément, ces règles fournissent comment la cyber assurance numérique est réalisée dans toute la République togolaise, en définissant les rôles et les responsabilités des principales parties prenantes pour la stratégie, la planification, le développement, la mise en œuvre et le suivi continu des performances de ces règles d'assurance.

Les règles fournissent également comme point de référence des contrôles de cybersécurité communs pour se défendre contre les menaces courantes qui exploitent les vulnérabilités connues en matière de cybersécurité et minimisent le risque d'exploitation pour les vulnérabilités non encore découvertes ou autrement connues sous le nom de vulnérabilités Zero day.

Ces règles de cybersécurité font partie des éléments essentiels de la stratégie nationale de cybersécurité de la République togolaise portée par l'ANCy.

G1 – Gouvernance, gestion et leadership

Ce domaine décrit les exigences de gouvernance requises pour les OSE en matière de règles de cybersécurité. Il s'agit d'améliorer davantage la responsabilisation en matière de cybersécurité et de promouvoir la visibilité globale requise de l'OSE.

Il s'agit également de faciliter l'atteinte des objectifs de cybersécurité et de fournir un niveau optimal de gestion des risques de cybersécurité.

Le domaine garantit en outre que la stratégie de sécurité doit être alignée sur la stratégie commerciale globale et assurer l'alignement et la conformité aux exigences de l'industrie, ainsi qu'aux lois et réglementations applicables.

Les contrôles et sous-contrôles suivants doivent être implémentés par tous les OSE.

G1.1	Leadership et engagement de la direction	
Objectif	Définir les rôles et les responsabilités de toutes les parties prenantes en vue de défendre et de renforcer la posture de cybersécurité de l'OSE.	
Contrôle	Faire preuve de leadership et d'engagement en matière de cybersécurité	
Sous-contrôles	G1.1.1	Conseil d'administration
		Le conseil d'administration est globalement responsable de l'état de la cybersécurité de l'OSE et doit recevoir des mises à jour régulières sur l'état de la sécurité de l'information au moins une fois par an.
	G1.1.2	PDG/Directeur Général
		Le PDG / Directeur Général a la responsabilité d'accepter et d'approuver les exigences de cybersécurité ; d'appliquer les contrôles de cybersécurité pour l'ensemble du Système d'informations de l'OSE, de veiller à ce que les politiques, les processus et les normes de cybersécurité soient mis en œuvre à l'échelle de l'OSE.
	G1.1.3	Comité de direction de la cybersécurité
		Le comité de direction de la cybersécurité doit être établi sous la présidence du Directeur Général ou de son délégué. Le comité comprend les chefs de chaque division de l'OSE qui assument les rôles suivants :

		a) superviser la mise en œuvre du programme de cybersécurité de l'OSE b) promouvoir la culture de la cybersécurité et de la sécurité chez l'OSE c) suivre et surveiller les performances du programme de cybersécurité de l'OSE d) s'assurer que le programme de cybersécurité est conforme aux exigences légales applicables e) s'assurer que des ressources et des compétences adéquates sont disponibles pour exécuter le programme de cybersécurité.
	G1.1.4	Position en cybersécurité
		La position de la fonction de cybersécurité dans l'OSE est importante pour lui donner l'indépendance dans l'exécution de ses responsabilités et pour prévenir tout conflit d'intérêts. L'OSE évitera tout conflit d'intérêts en vue de la mise en place de la fonction cybersécurité. Idéalement, la fonction de cybersécurité devrait relever de la Direction Générale ou de l'entité de gestion des risques et non au sein des directions informatiques.
	G1.1.5	Rôle du Responsable de la Sécurité du Système d'Information (RSSI)
		Le RSSI doit être nommé pour chaque OSE et avoir la responsabilité de coordonner et d'exécuter la conformité à cette règle. L'OSE élabore et met en œuvre un plan de formation et de montée en compétences du RSSI qui comprend au minimum une formation "ISO/IEC/27001 Management de la sécurité de l'information" ou équivalente.
	G.1.1.6	Communication des coordonnées du RSSI
		L'OSE communique les coordonnées de son Responsable de la sécurité des systèmes d'information (RSSI) ou de son point de contact en cybersécurité à son autorité de tutelle sectorielle, à l'ANCy et à son délégataire dans un délai de six (6) mois à compter de la notification de sa désignation comme OSE, ainsi qu'après chaque mise à jour de ces données.
	G1.1.7	Salariés
		Tous les employés ont la responsabilité de respecter les politiques publiées et de respecter les exigences et les directives en matière de cybersécurité.

G1.2	Organisation de la cybersécurité	
Objectif	Identifier les fonctions et relations clés pour la bonne performance en matière de cybersécurité	
Contrôle	S'assurer que la visibilité de la cybersécurité et les relations pertinentes sont établies ou renforcées.	
Sous-contrôles	G1.2.1	Contact avec les autorités
		L'OSE maintien des contacts appropriés et applicables avec les autorités, y compris, sans s'y limiter, l'élaboration de politiques et de procédures à cette fin.
	G1.2.2	Dossier d'accréditation
		L'OSE maintient et tient à jour un dossier d'accréditation, soumis à un contrôle annuel après sa désignation comme OSE. Le dossier contient : a. l'analyse de risques et les objectifs de sécurité pour les IE ; b. les procédures et les mesures de sécurité appliquées aux IE ; c. les risques résiduels, les mesures de réduction de ces risques et les raisons justifiant leur acceptation.
	G1.2.3	Contact avec les groupes d'intérêts spéciaux
		Des contacts appropriés avec des groupes d'intérêts spéciaux ou d'autres forums spécialisés dans la sécurité et des associations professionnelles doivent être établies ou renforcées.
	G1.2.4	La cybersécurité dans la gestion de projet
		Un responsable cybersécurité doit être présent dans toutes les fonctions de gestion de projet et faire partie des contributeurs, des examinateurs et des approbateurs avant l'achèvement du projet.
	G1.2.5	Séparation des tâches
		Les tâches et les domaines de responsabilité conflictuels doivent être examinés et séparés afin de réduire les possibilités de modification ou d'utilisation abusives ou non autorisées des actifs de l'OSE et de l'infrastructure essentielle.
	G1.2.6	Rôles et responsabilités en matière de cybersécurité
		Tous les rôles et responsabilités en matière de cybersécurité doivent être définis et attribués aux personnes appropriées.

G2 - Politique de sécurité et Plan de Sécurité d'Opérateur (PSO)

Les politiques de sécurité de l'information sont une partie importante des activités visant à établir des règles et des lignes directrices pour des fonctionnalités numériques efficaces afin de protéger les actifs de l'OSE et de ses infrastructures essentielles.

Les politiques fourniront un cadre, une orientation de gestion et un soutien en matière de cybersécurité pour l'OSE conformément aux exigences opérationnelles et aux lois et règlements applicables.

G2.1	Direction de gestion de la cybersécurité	
Objectif	Avoir des directives sur les pratiques de sécurité de l'information régissant les activités et les opérations des OSE.	
Contrôle	Avoir une politique de cybersécurité	
Sous-contrôles	G2.1.1	Politique de cybersécurité
		La politique doit : a. être établie et documentée pour l'OSE b. être pertinente et appropriée pour l'OSE c. inclure des objectifs de cybersécurité d. inclure l'engagement de répondre à toutes les exigences en matière de cybersécurité e. être approuvée par le conseil d'administration ou le directeur général/chef de la direction selon les cas
	G2.1.2	Politiques de soutien en matière de cybersécurité
		L'OSE établira et communiquera à l'ANCy un ensemble de politiques de cybersécurité à l'appui qui traitent de tous les aspects de la cybersécurité inclus dans ce règlement, tels que : a. Contrôle d'accès b. Gestion d'actifs c. Continuité d'activités d. Conformité en matière de sécurité e. Gestion des communications et des opérations f. Politique des ressources humaines g. Développement de systèmes d'information h. Gestion des incidents de sécurité i. Informatique mobile j. Cadre environnemental et physique k. Échange d'informations l. Cybersécurité m. Utilisation acceptable d'Internet n. Organisation de la cybersécurité
	G2.1.3	Examen des politiques de cybersécurité
		Les politiques doivent être maintenues, révisées, mises à jour à intervalles annuels et lorsque des changements importants se produisent.
	G2.1.4	Communiquer les politiques de cybersécurité
		a. Les politiques doivent être communiquées à tout le personnel et une confirmation de reconnaissance doit être obtenue pour s'assurer que tout le personnel comprend les attentes en la matière. b. Les politiques doivent être écrites et peuvent être communiquées à des tiers ou des fournisseurs pour la conformité. c. La communication des politiques aux utilisateurs doit se faire sous une forme pertinente, accessible et compréhensible. d. Une formation et une connaissance suffisantes des politiques doivent être fournies au public visé pour faciliter la connaissance de leur contenu.

		e. Les politiques doivent également être partagées aux nouveaux employés au cours du processus d'intégration et obtenir leur acceptation desdites politiques.

G3 – Conformité, audit et performance

Ce domaine fournit des contrôles pour s'assurer que l'OSE reste conforme à ses directives de cybersécurité tout au long des périodes tout en exigeant des examens annuels fournissant des assurances de conformité.

G3.1	Conformité	
Objectif	Éviter les violations des obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information et de toute exigence de sécurité.	
Contrôle	Se conformer aux exigences légales, contractuelles et de cybersécurité	
Sous-contrôles	G3.1.1	Identification de la législation applicable et des exigences contractuelles
		Toutes les exigences législatives, réglementaires et contractuelles pertinentes et l'approche de l'organisation pour répondre à ces exigences doivent être explicitement identifiées, documentées et tenues à jour pour chaque système d'information de l'OSE.
	G3.1.2	Droits de propriété intellectuelle
		Des procédures appropriées doivent être mises en œuvre pour assurer le respect des exigences législatives, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de produits logiciels propriétaires.
	G3.1.3	Protection des documents
		Les dossiers doivent être protégés contre la perte, la destruction, la falsification, l'accès non autorisé et la divulgation non autorisée, conformément aux exigences législatives, réglementaires, contractuelles et commerciales.
	G3.1.4	Confidentialité et protection des données à caractère personnel
		La confidentialité et la protection des données à caractère personnel doivent être assurées conformément à la législation et à la réglementation pertinentes, le cas échéant.
	G3.1.5	Réglementation du contrôle cryptographique
		Les contrôles cryptographiques doivent être utilisés conformément à tous les accords, lois et règlements pertinents.
	G3.1.6	Politique de conformité
		Mettre en place une politique de conformité qui encadre les exigences de sécurité juridiques, techniques et de gestion auxquelles l'OSE doit se conformer. La politique devrait également fournir l'approche pour établir les exigences de conformité et les étapes possibles que l'OSE suivra pour répondre aux exigences identifiées.
	G3.1.7	Conformité aux politiques et normes de sécurité
		Le premier responsable de l'OSE doit soutenir et s'assurer que celui-ci respecte les politiques et les normes de cybersécurité.

		Les gestionnaires doivent examiner régulièrement la conformité aux exigences en matière de cybersécurité au sein de leurs services responsables et prendre des mesures correctives en cas de lacunes.

G3.2	Audits de cybersécurité	
Objectif	S'assurer que la sécurité de l'information est mise en œuvre et exploitée conformément aux politiques et procédures organisationnelles	
Contrôle	Effectuer des examens pour l'assurance de la cybersécurité	
Sous-contrôles	G3.2.1	Audit indépendant de cybersécurité
		L'approche de l'OSE à l'égard de la gestion de la sécurité de l'information et de sa mise en œuvre (c.-à-d. les objectifs de contrôle, les contrôles, les politiques, les processus et les procédures de sécurité de l'information) doit être examinée de façon indépendante à des intervalles planifiés ou lorsque des changements importants se produisent.
	G3.2.2	Conformité aux politiques et normes de sécurité
		Les responsables examinent régulièrement la conformité du traitement et des procédures de l'information dans leur domaine de responsabilité avec les politiques, normes et autres exigences de sécurité appropriées.
	G3.2.3	Audit de la conformité technique
		Les systèmes d'information doivent faire l'objet d'un examen régulier pour s'assurer qu'ils sont conformes aux politiques et aux normes de sécurité de l'information de l'OSE.

G3.3	Audit	
Objectif	S'assurer que le programme de cybersécurité de l'OSE et ses opérations font l'objet d'un audit indépendant afin de fournir une assurance de l'efficacité du programme de protection de l'institution.	
Contrôle	Effectuer un audit régulier des fonctions de cybersécurité à l'OSE	
Sous-contrôles	G3.3.1	Vérification interne
		L'OSE procède à des audits internes à intervalles réguliers afin de fournir des assurances sures : a. l'harmonisation du programme et des opérations de sécurité de cyber avec les pratiques exemplaires b. l'alignement et conformité aux exigences togolaises en matière de cybersécurité c. l'identification des risques découlant de l'évaluation et ceux ayant été traités et corrigés.
	G3.3.2	Audit externe/Assurance
		L'OSE procède régulièrement à une évaluation de la cybersécurité au moins une fois tous les deux ans par un fournisseur externe indépendant et réputé. L'évaluation devrait inclure des tests d'intrusion techniques de l'infrastructure OSE.

G3.4	Performances en matière de cybersécurité	
Objectif	Mettre en place des indicateurs de performance afin de déterminer l'efficacité du programme de cybersécurité au sein de l'OSE	
Contrôle	Élaborer des indicateurs de performance pour mesurer l'efficacité des programmes et des opérations de cybersécurité	
Sous-contrôles	G3.4.1	Indicateurs de performance
		L'OSE élabore et met en œuvre des indicateurs de performance clés pour mesurer la performance des mesures de cybersécurité, notamment : a. Nombre d'incidents de sécurité détectés et évités b. Nombre de risques identifiés et corrigés c. Progression des vulnérabilités identifiées et corrigées d. Respect des présentes règles de cybersécurité e. Performances par rapport au PSO etc.
	G3.4.2	Tableau de bord de cybersécurité
		L'OSE élabore un tableau de bord de cybersécurité mettant en évidence les indicateurs de performance clés dans les domaines de la cybersécurité. Le tableau de bord doit être examiné et approuvé par la haute direction ou le comité directeur de la cybersécurité.

G4 – Gestion des risques de cybersécurité

S'assurer que les risques liés à la sécurité de l'information dans l'OSE sont identifiés, évalués et que ces risques sont traités conformément aux exigences et aux objectifs de sécurité de l'information de l'OSE.

L'analyse des risques consiste à identifier les principaux scénarios pertinents de menaces potentielles ou d'actes intentionnels possibles visant à interrompre le fonctionnement de l'Infrastructure Essentielle ou à la détruire.

G4.1	Méthodologie d'évaluation des risques	
Objectif	Mettre en place un processus d'identification des risques et d'évaluation régulière des risques	
Contrôle	Élaborer et documenter une méthodologie d'identification et d'évaluation des risques	
Sous-contrôles	G4.1.1	Identification des risques
		L'OSE dispose d'un processus documenté d'identification des risques conformément aux politiques, normes et procédures de cybersécurité publiées.
	G4.1.2	Méthodologie d'évaluation des risques
		L'OSE élabore une méthodologie d'évaluation des risques qui s'aligne sur les exigences des programmes de cybersécurité ainsi que sur les meilleures pratiques mondiales.
	G4.1.3	Fréquence de l'évaluation des risques

		L'OSE détermine une fréquence d'évaluation des risques conforme à la stratégie et aux opérations organisationnelles, idéalement une évaluation des risques par an.
	G4.1.4	Déterminer les critères de risque acceptables
		Identifier les critères de risques acceptables pour l'OSE dans le cadre de la méthode d'évaluation des risques
	G4.1.6	Déterminer la portée de l'évaluation des risques
		La portée de l'évaluation des risques est définie en collaboration avec les parties prenantes concernées dont l'environnement doit être évalué dans le cadre de cet exercice.
	G4.1.7	Menaces et vulnérabilités
		L'OSE dans le cadre de la méthodologie d'évaluation des risques détermine les menaces et les vulnérabilités connexes.
	G4.1.8	Sensibilisation à l'évaluation des risques
		L'OSE sensibilise tous les intervenants et le personnel à l'évaluation des risques sur la méthodologie d'évaluation des risques.

G4.2	Évaluation du risque	
Objectif	Effectuer une évaluation régulière des risques conformément à la méthodologie approuvée	
Contrôle	Effectuer une évaluation régulière des risques	
Sous-contrôles	G4.2.1	Évaluation régulière des risques
		L'OSE effectue une évaluation régulière et détaillée des risques conformément à la méthodologie d'évaluation des risques approuvée.
	G4.2.2	Analyse et hiérarchisation des risques
		L'OSE analyse et hiérarchise les risques en fonction de leur criticité afin d'établir des plans et des contrôles de prévention.
	G4.2.3	Résultats de l'évaluation des risques
		Les résultats d'évaluation des risques doivent être documentés et communiqués à toutes les parties prenantes pour avis et observations.

G4.3	Traitement et atténuation des risques	
	Objectif : Mettre en place un processus de prévention et de traitement des risques.	
Contrôle	Traiter et à atténuer les risques	
Sous-contrôles	G4.3.1	Plan de traitement des risques
		Un contrôle et un plan appropriés de traitement des risques doivent être identifiés pour faire face aux risques découlant de l'exercice d'évaluation des risques.
	G4.3.2	Approuver le plan de traitement des risques
		Le plan de traitement des risques identifié doit être documenté et approuvé par la haute direction appropriée.
	G4.3.3	Examen du traitement des risques

		Le plan de traitement des risques doit contenir des indicateurs de performance et faire l'objet d'un examen sur une fréquence régulière d'au moins deux fois par an.

G4.4	Acceptation des risques	
	Objectif : Avoir un processus formel en place pour l'acceptation des risques	
Contrôle	Gérer les risques acceptés	
Sous-contrôles	G4.4.1	Gestion des risques non traités
		L'OSE doit mettre en place un processus pour documenter le risque non traité ainsi que les risques résiduels et détermine comment ces risques doivent être gérés à l'avenir. Les risques non traités doivent être documentés et approuvés par le comité de direction.
	G4.4.2	Renonciation aux risques
		L'OSE dispose d'un processus de renonciation aux risques dans le cadre duquel le risque non traité est réduit au minimum par des contrôles compensatoires et les risques résiduels sont documentés et examinés sur une base trimestrielle jusqu'à ce que le risque soit traité.

G5 – Ressources Humaines

La sécurité des ressources humaines est une partie importante de la portée globale de la cybersécurité, car l'erreur humaine est la source principale dans plus de 90 % des incidents de sécurité (clic sur un lien de malveillant, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées). Il est donc important de mener et de mettre en œuvre des processus et des procédures de sécurité des ressources humaines pour tous les OSE.

G5.1	Vérifications avant l'emploi	
Objectif	S'assurer que les employés et les sous-traitants comprennent leurs responsabilités et sont adaptés aux rôles pour lesquels ils sont considérés.	
Contrôle	Réaliser des vérifications des antécédents avant l'embauche du personnel	
Sous-contrôles	G5.1.1	Vérification des antécédents
		Les vérifications des antécédents de tous les candidats à l'emploi doivent être effectuées conformément aux lois, règlements et éthiques pertinents et sont proportionnelles aux exigences de l'OSE, à la classification des informations à consulter et aux risques présentés, le cas échéant.
	G5.1.2	Communication relative au personnel essentiel
		L'OSE communique à l'ANCy toute embauche de son personnel essentiel
	G5.1.3	Conditions d'emploi
		Les ententes contractuelles avec les employés et les sous-traitants doivent énoncer leurs responsabilités et celles de l'OSE en matière de sécurité de l'information.

G5.2	Vérifications pendant l'emploi	
	Objectif : S'assurer que les employés et les sous-traitants sont conscients et s'acquittent de leurs responsabilités en matière de sécurité de l'information.	
Contrôle	Faire adhérer les employés aux politiques et pratiques de cybersécurité	
Sous-contrôles	G5.2.1	Responsabilités de gestion
		La direction exige que tous les employés et sous-traitants appliquent la sécurité de l'information conformément aux politiques et procédures établies de l'OSE.
	G5.2.2	Sensibilisation, éducation et formation à la sécurité de l'information
		Tous les employés de l'OSE et, le cas échéant, les sous-traitants doivent recevoir une éducation et une formation ou une sensibilisation appropriée et des mises à jour régulières des politiques et procédures organisationnelles, selon ce qui est pertinent pour leur fonction. Plus précisément pour respecter les exigences ci-dessous : a. Sensibilisation et formation du personnel b. Le PSO présente un plan de sensibilisation et de formation du personnel incluant la direction de l'OSE, les services en charge des Ressources Humaines, de la communication interne et externe, du système d'information, les directions métiers. c. Ce plan de formation est adapté aux différents interlocuteurs, en fonction de leurs responsabilités et de leurs fonctions dans l'OSE et dans le cadre du PSO. d. Chaque utilisateur de l'OSE a, au minimum, une session de formation ou de sensibilisation annuelle. e. Les administrateurs du système d'information et le Personnel Essentiel sont régulièrement formés sur la maintenance des équipements, des logiciels et des services dont ils ont la responsabilité.
	G5.2.3	Processus disciplinaire
		Un processus disciplinaire officiel et communiqué doit être mis en place pour prendre des mesures contre les employés qui commettent une atteinte à la sécurité de l'information.
	G5.2.4	Disponibilité du Personnel Essentiel
		Le Personnel Essentiel de l'OSE doit être suffisamment disponible pour une fourniture continue et ininterrompue du ou des Service(s) Essentiel(s) de l'OSE. L'OSE communique à l'ANCy et/ou à son délégataire la liste de son Personnel Essentiel dans un délai de trois (3) mois à compter de la notification de sa désignation comme OSE, ainsi qu'après chaque mise à jour de ces coordonnées.

G5.3	Cessation d'emploi et changement d'emploi	
Objectif	Protéger les intérêts de l'OSE dans le cadre du processus de changement ou de cessation d'emploi	
Contrôle	Sécuriser la cessation ou le changement d'emploi	
Sous-contrôles	G5.3.1	Cessation d'emploi ou changement de responsabilités
		Les responsabilités et les obligations en matière de sécurité de l'information qui restent valables après la cessation d'emploi ou le changement d'emploi doivent être définies, communiquées à l'employé ou à l'entrepreneur et appliquées.
	G5.3.2	Communication relative au personnel essentiel
		L'OSE communique à l'ANCy toute cessation d'emploi de son personnel essentiel

G6 – Relation fournisseur

L'objectif de ce contrôle est de s'assurer que toutes les relations avec les fournisseurs sont exploitées et gérées de manière sécurisée afin de ne pas introduire de risques de sécurité pour l'OSE dans la conduite des affaires.

G6.1	Sécurisation des relations avec les fournisseurs	
Objectif	S'assurer que toutes les relations avec les fournisseurs sont sécurisées	
Contrôle	Avoir des accords et des processus avec les fournisseurs pour leur adhésion aux politiques de cybersécurité de l'OSE	
Sous-contrôles	G6.1.1	Politique relative aux relations avec les fournisseurs
		Les exigences en matière de sécurité des informations doivent être définies, documentées et convenues avec le fournisseur afin de minimiser les risques associés aux relations contractuelles avec ce dernier.
	G6.1.2	Accords avec les fournisseurs
		Toutes les exigences de sécurité doivent être documentées dans tous les accords.

G6.2	Gestion de la prestation de services	
Objectif	Avoir un niveau convenu de cybersécurité et de prestation de services	
Contrôle	S'assurer que les services convenus sont maintenus tout le temps	
Sous-contrôles	G6.2.1	Surveiller et examiner les services des fournisseurs
		Surveiller et examiner régulièrement les services des fournisseurs au moins une fois par an.
	G6.2.2	Changements aux services des fournisseurs
		Toute modification apportée aux services des fournisseurs doit être notifiée et gérée de manière à identifier les risques liés à la sécurité de l'information.

G6.3	Processus d'approvisionnement	
Objectif	S'assurer que toutes les relations avec les fournisseurs sont sécurisées et conformes aux réglementations et aux politiques de l'OSE	
Contrôle	Inclure la sécurité dans les accords avec les fournisseurs	
Sous-contrôles	G6.3.1	Obtention d'accords
		Les accords avec les fournisseurs doivent traiter des aspects liés : a. Au respect de l'environnement légal togolais dans tout contrat avec un fournisseur b. A la protection des données à caractère personnel c. A la protection des informations confidentielles concernant les IE d. A la situation financière du fournisseur au moment de la signature du contrat et à son actionnariat e. A la signature d'un accord de confidentialité avec des sanctions réelles en cas de violation, avant tout autre contrat f. Aux possibilités de transfert de droits d'auteur dans le cadre du développement de logiciels pour un droit de modifications du logiciel ou de développements ultérieurs de manière indépendante, ou au moins à un mécanisme de séquestre (notarié par exemple) concernant les codes sources et l'environnement de développement d'une application donnée g. A toutes solutions, organisationnelles, matérielles et techniques concernant la continuité de services du fournisseur en cas d'une défaillance de ce dernier h. Aux règles de suppression des erreurs signalées, sous forme « d'accord de niveau de service » (SLA – Service-Level Agreement), avec procédures de coopération pour une suppression en temps voulu des erreurs signalées, et sanction pour retards ou non-suppression i. Au partenariat en cas de détection de nouvelles vulnérabilités des logiciels fournis par un éditeur avec un "accord de niveau de service" (SLA – Service-Level Agreement) j. A l'accès au code source, pendant toute la durée du contrat et après sa résiliation, par l'OSE ou à l'auditeur choisi par les parties, concernant les logiciels critiques pour les IE de l'OSE k. Aux dispositions sur la procédure de gestion des modifications d'un logiciel et le mode de rémunération du prestataire de services l. Aux dispositions relatives aux mécanismes de sanctions au bénéfice de l'OSE à l'encontre d'un fournisseur en cas de violation de ses obligations. L'objectif est que les sanctions soient à la hauteur des responsabilités du fournisseur et des risques pour l'OSE m. A l'obligation du fournisseur de souscrire à une police d'assurance contre les dommages causés par une mauvaise exécution du contrat. n. A une procédure permettant de prendre des mesures immédiates en cas de menaces pour la fourniture d'un service essentiel résultant d'attaques contre l'Infrastructure Essentielle

		o. A une procédure de voie d'escalade formalisée pour résoudre des problèmes découlant de l'exécution du contrat

G6.4	Logiciel acheté	
Objectif	Protéger les logiciels achetés	
	Prendre des dispositions renforçant la sécurité contre les menaces des logiciels fournis, y compris notamment, de systèmes d'automatisation ou de contrôle industriel	
Contrôle	S'assurer de la mise en place d'un mécanisme adéquat pour couvrir les risques liés aux logiciels achetés	
Sous-Contrôle	G6.4.1	S'assurer qu'il n'y a pas de faille de sécurité dans les logiciels fournis
		L'obligation du fournisseur de vérifier que le logiciel fourni ne présente pas de lacunes de sécurité connues et d'informer l'OSE de toute lacune existante.
	G6.4.2	Correction des vulnérabilités logicielles
		La déclaration que l'architecture du logiciel fourni permet de supprimer les éventuelles failles de sécurité qui seront détectées pendant le cycle de vie du logiciel.
	G6.4.3	Composants logiciels
		La liste de tous les composants du logiciel fourni est jointe au contrat.
	G6.4.4	Déclaration du fournisseur sur le logiciel fourni
		L'éditeur de logiciels met à la disposition une déclaration sur les règles qu'il applique pour combler les lacunes de sécurité détectées, les règles d'information des utilisateurs sur les lacunes de sécurité détectées et les règles de distribution des correctifs.

P1 – Contrôle d'accès

Pour garantir des contrôles d'accès sécurisés, des politiques et des procédures sont mises en place et appliquées aux utilisateurs, aux réseaux, aux systèmes, aux applications et aux systèmes d'exploitation afin de prévenir ou de minimiser les tentatives et les accès non autorisés.

P1.1	Exigences métiers pour le contrôle d'accès	
Objectif	Contrôler l'accès aux systèmes d'information et de traitement de l'information au niveau de l'utilisateur, de l'application, du réseau et du système d'exploitation, y compris l'informatique mobile ainsi que les procédures d'autorisation des actifs informationnels.	
Contrôle	Contrôler l'accès aux ressources de l'OSE	
Sous-contrôles	P1.1.1	Politique de contrôle d'accès
		La politique de contrôle d'accès doit être mise en place et documentée en fonction des exigences métiers et de cybersécurité.
	P1.1.2	Accès aux systèmes, aux réseaux et aux applications
		Accès aux réseaux, aux systèmes et aux infrastructures essentielles uniquement après autorisation.

P1.2	Gestion de l'accès des utilisateurs	
Objectif	Assurer l'accès autorisé des utilisateurs et empêcher l'accès non autorisé aux systèmes et services	
Contrôle	Gérer les exigences d'accès des utilisateurs	
Sous-contrôles	P1.2.1	Enregistrement et radiation de l'utilisateur
		Un processus formel d'enregistrement et de radiation des utilisateurs est mis en œuvre pour permettre l'attribution des droits d'accès.
	P1.2.2	Provisionnement de l'accès utilisateur
		Un processus documenté de provisionnement de l'accès des utilisateurs doit être mis en œuvre pour attribuer ou révoquer les droits d'accès pour tous les types d'utilisateurs à tous les systèmes et services.
	P1.2.3	Gestion des droits d'accès privilégiés
		L'attribution et l'utilisation des droits d'accès privilégiés sont restreintes et contrôlées sur la base du principe du « need to know et du need to have ». Les droits d'accès privilégiés ne sont accordés qu'aux personnes qui en fonction de leurs positions et de leurs rôles en un moment donné en ont réellement besoin.
	P1.2.4	Gestion des informations d'authentification restreintes des utilisateurs
		L'attribution d'informations d'authentification restreintes doit être contrôlée au moyen d'un processus documenté.
	P1.2.5	Examen régulier des droits d'accès des utilisateurs
		Les propriétaires d'actifs doivent examiner les droits d'accès des utilisateurs à intervalles réguliers.
	P1.2.6	Suppression ou ajustement des droits d'accès

		Les droits d'accès de tous les employés et utilisateurs externes aux installations de traitement de l'information doivent être supprimés à la cessation de leur emploi ou de leur contrat ou ajustés en cas de modification.

P1.3	Responsabilités de l'utilisateur	
Objectif	Assurer la responsabilisation à l'égard de la protection des renseignements d'authentification des utilisateurs	
Contrôle	Protéger les informations d'authentification des utilisateurs	
Sous-contrôles	P1.3.1	Utilisation des informations d'authentification restreinte
		Les utilisateurs doivent respecter les exigences et les pratiques de cybersécurité de l'OSE en ce qui concerne l'utilisation des informations secrètes d'authentification.

P1.4	Contrôle d'accès aux systèmes et aux applications	
Objectif	Empêcher l'accès non autorisé aux systèmes et applications	
Contrôle	Restreindre l'accès aux systèmes et aux applications	
Sous-contrôles	P1.4.1	Restrictions d'accès aux informations
		L'accès aux fonctions de l'information et du système d'application est limité conformément à la politique de contrôle d'accès.
	P1.4.2	Procédures de connexion sécurisées
		Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée.
	P1.4.3	Système de gestion des mots de passe
		Les systèmes de gestion des mots de passe sont interactifs et garantissent la qualité des mots de passe.
	P1.4.4	Utilisation de programmes utilitaires privilégiés
		L'utilisation de programmes utilitaires susceptibles de contourner les contrôles du système et des applications doit être restreinte et étroitement contrôlée.
	P1.4.5	Contrôle d'accès au code source
		L'accès au code source des logiciels développés en internes doivent être restreint et diffusé seulement sur la base du principe du « need to know et du need to have ».
	P1.4.6	Authentification
		Tous les systèmes de l'OSE sont accessibles via des mécanismes d'authentification où des noms d'utilisateur et des mots de passe sont utilisés pour accéder aux systèmes. Une authentification multi facteur supplémentaire sera déployée pour tous les accès aux systèmes critiques ainsi que l'accès aux informations sensibles.
	P1.4.7	Comptes par défaut du fournisseur

		Tous les comptes et mots de passe par défaut du fournisseur doivent être remplacés par les comptes uniques de l'OSE conformément à la stratégie de mot de passe (sous-contrôle 4.4.9).
	P1.4.8	Les éléments secrets d'authentification
		Les éléments secrets d'authentification sont modifiés par l'OSE chaque fois que cela est nécessaire, entre autres : a. Suite à l'installation par le fabricant ou le fournisseur d'une ressource, avant sa mise en service. b. à chaque retrait d'un utilisateur d'un compte commun de plusieurs utilisateurs. c. en cas de suspicion de compromission. d. trimestriellement (au maximum). Quand un élément secret ne peut pas être modifié, l'OSE met en place un contrôle d'accès approprié à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe. Les utilisateurs qui n'en ont pas la responsabilité ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair.
	P1.4.9	Mot de passe en tant que données d'authentification
		Lorsque les éléments secrets d'authentification sont des mots de passe : a. L'OSE a une politique de construction de mots de passe "forts" et définit la complexité (types de caractères) et la longueur minimale de ces mots de passe, tout en prenant en compte les limites permises par la ressource concernée. L'OSE met en place, autant que possible, des mécanismes de contrôles des règles définies, et les documente. b. L'OSE s'assure que les mots de passe temporaires attribués à un utilisateur sont uniques et qu'ils sont modifiés lorsqu'ils sont utilisés pour la première fois. c. Lors du transfert d'un mot de passe, il convient d'utiliser un canal de communication différent de celui utilisé pour le transfert d'un identifiant, par exemple l'identifiant par courrier électronique et le mot de passe par SMS, MMS, Messagerie instantanée, ou autre canal de communication approprié. d. L'OSE vérifie que les utilisateurs ne puissent pas réutiliser le même mot de passe entre plusieurs comptes, avec une particulière attention sur les comptes privilégiés. e. Dans le cadre de la sauvegarde des mots de passe, seules les "hash" sont conservés et dans les cas où il est nécessaire de récupérer un mot de passe, il doit être conservé dans une enveloppe sécurisée dans un coffre.
	P1.4.10	Accès à distance
		Lorsque l'accès à l'IE est effectué depuis un site extérieur à celui de l'OSE : a. il doit être protégé par des mécanismes de chiffrement et d'authentification, des solutions de chiffrement de la

		transmission des données, telles que VPN, SSH ou autres, afin d'éviter les écoutes et l'interception des informations ; b. le mécanisme d'authentification est renforcé en mettant en œuvre une authentification à double facteur (authentification impliquant à la fois un élément secret et un autre élément propre à l'utilisateur), sauf si des raisons techniques ou opérationnelles ne le permettent pas, ce qui doit être documenté le cas échéant ; c. toutes les sessions d'accès à distance doivent être automatiquement enregistrées. Cela s'applique aux employés et aux prestataires de services (tel que le personnel technique externe) ; d. les mémoires de masse de ces équipements doivent être en permanence protégées par des mécanismes de chiffrement et d'authentification.

P2 – Gestion des actifs

Il s'agit d'une part de s'assurer que tous les actifs sont référencés et inclus dans les programmes de sécurité et d'autre part d'assurer la protection des actifs informationnels et leur classification.

Ce domaine fournit des assurances contre les actifs non autorisés à placer dans l'environnement de l'OSE, fournit un processus visant à maintenir la responsabilité lors de la gestion, et du traitement des informations organisationnelles et des actifs d'infrastructure.

P2.1	**Responsabilité des actifs**	
Objectif	Identifier les actifs de l'OSE et définir la protection et les responsabilités appropriées	
Contrôle	Gérer les actifs	
Sous-contrôles	P2.1.1	Cartographie des actifs
		L'OSE réalise l'inventaire des actifs pour son IE à la fois logiciel et matériel.
	P2.1.2	Propriété des actifs
		Tous les actifs doivent être attribués à un propriétaire spécifié avec des responsabilités de gestion pour chaque actif identifié.
	P2.1.3	Utilisation acceptable des biens
		L'OSE doit identifier les règles régissant l'utilisation des actifs informationnels. Ces règles doivent être identifiées, documentées et mises en œuvre.
	P2.1.4	Rendement des actifs
		L'OSE met en place un processus pour tous les utilisateurs, le personnel et les sous-traitants qui détiennent des actifs de l'OSE à retourner à la fin de leurs engagements. La restitution des ressources doit également être effectuée en cas de changement d'emploi ou lorsque l'employé cesse d'utiliser la ressource dans l'exercice de ses fonctions.

P2.2	Classification des actifs	
Objectif	S'assurer que les actifs informationnels bénéficient d'un niveau de protection approprié	
Contrôle	Classifier les actifs	
Sous-Contrôle	P2.2.1	Classification des actifs informationnels
		Les OSE classent leurs informations en fonction de la sensibilité de l'accès ou de la divulgation non autorisés.
	P2.2.2	Étiquetage des informations
		Des procédures d'étiquetage conformes à la classification des actifs sont élaborées.
	P2.2.3	Gestion des actifs
		Ces procédures sont utilisées pour la manipulation des actifs conformément au système de classification des actifs.

P2.3	Gestion des médias	
Objectif	Empêcher la modification, la suppression, la divulgation ou la destruction non autorisées d'informations stockées dans un média	
Contrôle	Avoir des processus et des procédures pour la gestion des médias	
Sous-contrôles	P2.3.1	Gestion des supports de suppression
		L'OSE devra mettre en place des procédures documentées pour la suppression des supports médias conformément au système de classification.
	P2.3.2	Cession des supports
		Les supports doivent être éliminés en toute sécurité lorsqu'ils ne sont plus nécessaires.
	P2.3.3	Transfert de support physique
		Les OSE doivent mettre en place des procédures et des équipements pour protéger les supports contenant des informations contre l'accès non autorisé, l'utilisation abusive ou la corruption pendant le transport.

P2.4	Politique de gestion des actifs	
Objectif	Disposer d'une politique pour diriger et guider les OSE ayant un processus et une pratique de gestion des actifs	
Contrôle	Avoir une politique de gestion des actifs documentée	
Sous-contrôles	P2.4.1	Contenu de la politique
		La politique de gestion des actifs doit : a) Refléter et être approprié aux actifs des OSE b) Fournir un cadre et une structure sur la gestion des actifs c) Responsabiliser des personnes dans la gestion des actifs

		d) S'aligner sur d'autres politiques de cybersécurité et directives de cybersécurité en matière de la gestion des actifs

P2.5	Gestion des équipements personnels (BYOD – Bring Your Own Device)	
Objectif	Faciliter l'intégration des équipements et des terminaux personnels (Bring Your Own Device) de manière sécurisée tout en accédant aux ressources d'information des OSE.	
Contrôle	Elaborer des règles régissant l'utilisation sécurisées des équipements personnels	
Sous-contrôles	P2.5.1	Utilisation acceptable du BYOD
		Les règles acceptables sur l'utilisation du BYOD doivent être documentées et communiquées. Utilisation de contrôles techniques à adopter pour faire respecter les règles d'utilisation du BYOD.
	P2.5.2	Séparation des informations personnelles avec celles des OSE
		L'accès à l'information doit être séparé entre les données personnelles et les données de l'OSE.
	P2.5.3	Accès BYOD basé sur les rôles (fonctions)
		Définir l'accès BYOD en fonction des différents rôles et pour des besoins de traçabilité.

P3 – Sécurité des communications

Sécuriser les canaux de communication, y compris l'infrastructure sous-jacente entre diverses organisations, ainsi que les communications internes au sein de l'OSE.

Ce domaine répond également aux exigences relatives à la sécurisation de l'information en transit ainsi qu'au partage de l'information entre divers OSE et individus. Cela assure en outre la présence de contrôles pour protéger l'échange d'informations.

P3.1	Contrôles de sécurité réseau	
	Objectif : Assurer la protection de l'information dans les réseaux et ses moyens de traitement	
Contrôle	Gérer et contrôler les réseaux pour protéger les informations contenues dans les systèmes et les applications.	
Sous-contrôles	P3.1.1	Contrôles réseau
		Les réseaux sont gérés et contrôlés pour protéger les informations stockées, traitées et transmises dans les systèmes et les applications.
	P3.1.2	Sécurité des services réseau
		Les mécanismes de sécurité, les niveaux de service et les exigences de gestion de tous les services de réseau doivent être identifiés et inclus dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
	P3.1.3	Ségrégation dans les réseaux

		Les groupes de services d'information, d'utilisateurs et de systèmes d'information sont séparés sur les réseaux.

P3.2	Transfert d'informations	
	Objectif : Maintenir la sécurité des informations transférées au sein d'un OSE et avec toute entité externe	
Contrôle	Contrôler et sécuriser les flux d'informations	
Sous-contrôles	P3.2.1	Politiques et procédures de transfert de l'information
		Des politiques, des procédures et des contrôles formels en matière de transfert doivent être mises en place pour protéger le transfert d'information par l'utilisation de tous les types d'installations de communication.
	P3.2.2	Accords sur le transfert d'informations
		Les ententes portent sur le transfert sécurisé d'informations sensibles entre l'OSE et les parties externes.
	P3.2.3	Messagerie électronique
		Les informations contenues dans la messagerie électronique doivent être protégées de manière appropriée.
	P3.2.4	Accords de confidentialité ou de non-divulgation
		Les exigences en matière d'ententes de confidentialité ou de non-divulgation reflétant les besoins de l'OSE en matière de protection de l'information doivent être identifiées, régulièrement examinées et documentées.

P3.3	Filtrage réseau	
Objectif	Filtrer le trafic réseau non autorisé et autoriser uniquement le trafic requis à traverser le réseau OSE	
Contrôle	Filtrer le trafic réseau non autorisé	
Sous-contrôles	P3.3.1	Filtrage du flux de données
		L'opérateur de services essentiels met en place des mécanismes de filtrage des flux de données circulant dans ses Infrastructures Essentielles et avec les infrastructures tierces afin de bloquer la circulation de flux non strictement nécessaires au fonctionnement de ses infrastructures et pour l'ensemble des systèmes.
	P3.3.2	Documentation des règles de filtrage
		Une documentation à jour doit faire part des règles de filtrage mises en place pour chaque IE ainsi que des risques acceptés par l'OSE et des mesures supplémentaires de réduction du risque que l'OSE met en place.
	P3.3.3	Paramètres de filtrage
		L'OSE définit les règles de filtrage des flux de données (filtrage sur les adresses réseau, sur les protocoles, sur les numéros de port, etc.) afin

		de limiter la circulation des flux de données nécessaires au fonctionnement et à la sécurité de ses IE.
	P3.3.4	Solution de filtrage à mettre en place
		L'OSE précise les solutions de filtrage telles que pare-feu ou division en VLAN utilisées pour l'optimisation du filtrage et de la séparation du trafic entrant et sortant des IE, ainsi que sur les flux entre les sous-systèmes des IE.
	P3.3.5	Empêcher l'accès direct à Internet
		Les IE de l'OSE n'ont pas d'accès direct à internet. Les ressources matérielles et logicielles des IE de l'OSE ne sont pas directement connectées à Internet. Elles passent par un pare-feu-passerelle (gateway firewall) de dernière génération pour empêcher des connexions réseau sortantes et sont séparées des serveurs DNS, des serveurs de courrier électronique et des serveurs proxy.
	P3.3.6	Avoir mis en place des procédures d'enregistrement, de surveillance et de blocage
		L'OSE met en œuvre les procédures d'enregistrement, de surveillance et de blocage des accès aux adresses IP nuisibles, aux publicités et aux réseaux anonymes. La catégorisation (liste blanche) des types de contenu de réseau et des sites ayant une bonne réputation est mise en place et documentée.
	P3.3.7	Par défaut, bloquer le trafic non requis
		Par défaut, l'OSE bloque tout trafic réseau (entrant ou sortant) inutile et non autorisé – y compris celui généré par des applications non fiables – par l'utilisation de solutions adéquates telles que des IPS/IDS ou des pare-feu applicatifs (Web Application Firewall ou WAF).
	P3.3.8	Filtrage et contrôle DNS
		L'OSE ne permet la connexion qu'aux seuls serveurs DNS de confiance et un filtrage détaillé des requêtes DNS doit être effectué.

P3.4	Protection des e-mails	
Objectif	Protéger les messages électroniques et les communications avec l'extérieur	
Contrôle	Protéger le trafic de messagerie et le système	
Sous-contrôles	P3.4.1	Avoir une stratégie et un plan de protection des e-mails documentés
		L'OSE élabore, met en œuvre et documente son plan de protection des messages électroniques–pour se protéger contre les courriels d'hameçonnage, d'harponnage (phishing, spear phishing) ainsi que les possibilités d'usurpation d'identités, principaux vecteurs d'attaques informatiques.
	P3.4.2	Compte de messagerie individuel pour tout le personnel
		Chaque utilisateur de l'OSE a une adresse de courrier électronique, propriété de l'OSE, contrôlée par l'OSE.
	P3.4.3	Limitation de l'utilisation des e-mails personnels
		L'utilisation d'autres adresses de courrier électronique par l'utilisateur (notamment adresses emails personnelles) n'est pas accessible sur les infrastructures informatiques de l'OSE. Tout cas

		contraire est justifié, documenté, et des mécanismes de traçabilité sont mis en place pour réduire le niveau de risque lié à cette utilisation.
	P3.4.4	Sensibilisation à l'utilisation et à la protection des e-mails
		L'OSE met en œuvre son plan d'éducation des utilisateurs à l'utilisation de la messagerie électronique d'entreprise, moyen de base pour protéger ses IE. Cette éducation comprend entre autres : a) Les moyens d'identifier et d'éviter les courriels d'hameçonnage (par exemple avec des liens pour se connecter à de fausses pages) ; b) L'explication et l'incitation à l'utilisation des adresses de courrier électronique fournies par l'OSE à l'utilisateur dans le cadre de ses fonctions.
	P3.4.5	Protection des e-mails contre les menaces connues et inconnues
		L'OSE définit, met en œuvre et documente les procédures appropriées afin : a. D'isoler du contenu du réseau (sandboxing) par un blocage en cas de comportement suspect, par exemple basé sur le trafic réseau, les fichiers nouveaux ou modifiés et autres changements inhabituels du système ; b. D'utiliser une catégorisation des types de pièces jointes autorisées (liste blanche), interdites (liste noire), y compris les archives et les archives imbriquées, et protégées par un mot de passe ; c. D'analyser/nettoyer les liens, les fichiers PDF et de passer les macros Microsoft Office ou leur configuration par une période de quarantaine ; d. D'utiliser le "Sender Policy Framework" ou le "Sender ID" pour vérifier les courriers électroniques entrants ; e. D'utiliser les méthodes "SPF TXT hard fail", les enregistrements "DNS DMARC" et les enregistrements "DNS DKIM" (DomainKeys Identified Mail) pour bloquer les courriers électroniques se faisant passer pour des courriers électroniques de votre propre organisation ; f. De bloquer les services de cloud computing non fiables/non approuvés ; g. D'enregistrer les destinataires, la taille, le nombre et la fréquence des e-mails envoyés ; h. De bloquer les messages contenant des pièces jointes sous forme de fichiers exécutables.
	P3.4.6	Chiffrement des e-mails
		L'OSE élabore, met en œuvre et documente des mécanismes de chiffrement puissants utilisés entre les serveurs de courrier électronique ou pour protéger le courrier électronique lui-même.
	P3.4.7	Protection des transactions
		Les informations sur les détails des transactions ne doivent pas être disponibles sur les réseaux publics.

REGLES DE CYBERSECURITE

P3.5	Comptes d'administration – Limitation et supervision des droits d'accès privilégiés	
Objectif	Prévenir les abus ou l'accès non autorisé aux comptes privilège	
Contrôle	Disposer d'un processus de protection des comptes à privilège	
Sous-contrôles	P3.5.1	Gestion de compte privilège
		L'OSE définit, conformément à son PSO, les règles de gestion et d'attribution des comptes privilégiés liés à ses Infrastructures Essentielles.
	P3.5.2	Procédures pour les modifications de compte à privilège
		La procédure de modification (ajout, suppression, suspension ou modification des droits associés) sur les comptes privilégiés, inclut une vérification stricte des droits, pour s'assurer que seuls les droits strictement nécessaires sont accordés en cohérence avec les besoins d'utilisation de chaque compte.
	P3.5.3	Allocation documentée des comptes à privilège avec les droits respectifs
		Une documentation des comptes privilégiés et des droits associés est établie et maintenue, indiquant l'ensemble des comptes et droits privilégiés existants liés aux IE, ainsi que toutes les fonctions privilégiées concernant les IE, toutes les procédures et fonctions de protection mises en place et décrivant les risques existants, acceptés et gérés. La liste des comptes privilégiés des IE est systématiquement maintenue.
	P3.5.4	Affectations de privilège minimales
		Suivant la définition de ses fonctions, chaque utilisateur ayant des droits privilégiés, principalement pour l'administration des systèmes doit avoir, autant que possible, des droits strictement restreints au périmètre fonctionnel et technique dont il est responsable.
	P3.5.5	Comptes administratifs privilégiés
		Les droits d'accès privilégiés, principalement pour l'administration, sont identifiés par système ou par processus, et par utilisateur auquel ils sont accordés.
	P3.5.6	Allocation de compte de privilège de l'administrateur minimum
		Les privilèges d'administrateur pour les systèmes d'exploitation, les bases de données et les applications sont limités au minimum nécessaire, en fonction des tâches à effectuer.
	P3.5.7	Droits du personnel privilégié
		Les droits accordés aux employés privilégiés, dont les administrateurs, doivent être divisés en trois comptes : a. Compte d'utilisateur – Compte personnel ; b. Compte d'administrateur local – Compte d'assistance aux utilisateurs ; c. Compte d'administrateur sur les serveurs - Compte d'administration des serveurs.

REGLES DE CYBERSECURITE

P3.5	Comptes d'administration – Limitation et supervision des droits d'accès privilégiés	
Objectif	Prévenir les abus ou l'accès non autorisé aux comptes privilège	
Contrôle	Disposer d'un processus de protection des comptes à privilège	
Sous-contrôles	P3.5.1	Gestion de compte privilège
		L'OSE définit, conformément à son PSO, les règles de gestion et d'attribution des comptes privilégiés liés à ses Infrastructures Essentielles.
	P3.5.2	Procédures pour les modifications de compte à privilège
		La procédure de modification (ajout, suppression, suspension ou modification des droits associés) sur les comptes privilégiés, inclut une vérification stricte des droits, pour s'assurer que seuls les droits strictement nécessaires sont accordés en cohérence avec les besoins d'utilisation de chaque compte.
	P3.5.3	Allocation documentée des comptes à privilège avec les droits respectifs
		Une documentation des comptes privilégiés et des droits associés est établie et maintenue, indiquant l'ensemble des comptes et droits privilégiés existants liés aux IE, ainsi que toutes les fonctions privilégiées concernant les IE, toutes les procédures et fonctions de protection mises en place et décrivant les risques existants, acceptés et gérés. La liste des comptes privilégiés des IE est systématiquement maintenue.
	P3.5.4	Affectations de privilège minimales
		Suivant la définition de ses fonctions, chaque utilisateur ayant des droits privilégiés, principalement pour l'administration des systèmes doit avoir, autant que possible, des droits strictement restreints au périmètre fonctionnel et technique dont il est responsable.
	P3.5.5	Comptes administratifs privilégiés
		Les droits d'accès privilégiés, principalement pour l'administration, sont identifiés par système ou par processus, et par utilisateur auquel ils sont accordés.
	P3.5.6	Allocation de compte de privilège de l'administrateur minimum
		Les privilèges d'administrateur pour les systèmes d'exploitation, les bases de données et les applications sont limités au minimum nécessaire, en fonction des tâches à effectuer.
	P3.5.7	Droits du personnel privilégié
		Les droits accordés aux employés privilégiés, dont les administrateurs, doivent être divisés en trois comptes : a. Compte d'utilisateur – Compte personnel ; b. Compte d'administrateur local – Compte d'assistance aux utilisateurs ; c. Compte d'administrateur sur les serveurs - Compte d'administration des serveurs.

	P3.5.8	Utilisation des comptes à privilège
		Les comptes privilégiés sont exclusivement utilisés pour des activités professionnelles impliquant des droits d'accès privilégiés. De même, les accès privilégiés sont exclusivement réalisés par des comptes privilégiés.
	P3.5.9	Authentification de compte à privilège
		L'authentification multi-facteur est utilisée pour tous les utilisateurs aux droits d'accès privilégiés par accès à distance (à partir de réseaux externes).
	P3.5.10	Pistes d'audit de compte privé et utilisation de la solution PAM
		Des mesures de traçabilité, des fonctions privilégiées dont celles d'administration, ainsi que des comptes privilégiés sont mises en place. La restriction de l'accès des utilisateurs aux seuls systèmes et ressources dont ils ont besoin et la mise en œuvre des exigences relatives à la gestion des accès privilégiés sont facilitées par les solutions PAM (Privileged Access Management).
	P3.5.11	Audit annuel du compte de privilège
		La tenue des comptes privilégiés est auditée dans le cadre de la procédure d'accréditation annuelle.

P4 – Systèmes d'information, acquisition et maintenance

Ce domaine énumère les contrôles nécessaires pour sécuriser le processus d'acquisition, de développement et de maintenance des systèmes afin d'éviter l'utilisation abusive des informations ou la modification non autorisée et d'élever les niveaux de sécurité dans les applications, pendant le développement, ainsi que pour traiter les vulnérabilités techniques.

Le domaine intègre davantage les exigences de cybersécurité au développement du cycle de vie des systèmes et des applications.

P4.1	Exigences de sécurité des systèmes d'information	
Objectif	S'assurer que la sécurité de l'information fait partie intégrante des systèmes d'information tout au long du cycle de vie. Cela inclut également les exigences applicables aux systèmes d'information qui fournissent des services sur les réseaux publics.	
Contrôle	Sécuriser les systèmes de traitement des informations	
Sous-contrôles	P4.1.1	Analyse et spécifications des exigences en matière de sécurité de l'information
		Les exigences relatives à la sécurité de l'information sont incluses dans les exigences relatives à l'acquisition de nouveaux systèmes d'information ou aux améliorations apportées aux systèmes d'information existants.
	P4.1.2	Sécurisation des services applicatifs sur les réseaux publics
		Les informations impliquées dans les services applicatifs passant sur les réseaux publics doivent être protégées contre les activités

		frauduleuses, les litiges contractuels, la divulgation et la modification non autorisées.
	P4.1.3	Protection des transactions des services applicatifs
		Les informations impliquées dans les transactions de service d'application doivent être protégées afin d'éviter une transmission incomplète, un mauvais routage, une altération non autorisée des messages, une divulgation non autorisée, une duplication ou une relecture non autorisée des messages.

P4.2	Sécurité dans les processus de développement et de support	
Objectif	S'assurer que la sécurité de l'information est conçue et mise en œuvre dans le cycle de vie de développement des systèmes d'information	
Contrôle	S'assurer que la cybersécurité est intégrée dans les systèmes et le développement d'applications	
Sous-contrôles	P4.2.1	Politique de développement sécurisée
		Les règles pour le développement de logiciels et de systèmes doivent être établies et appliquées aux développements au sein de l'OSE.
	P4.2.2	Procédures de contrôle des modifications du système
		Les modifications apportées aux systèmes au cours du cycle de vie du développement doivent être contrôlées par l'utilisation de procédures formelles de contrôle des modifications.
	P4.2.3	Examen technique des applications après des modifications de la plate-forme d'exploitation
		Lorsque les plates-formes d'exploitation sont modifiées, les applications critiques de l'OSE doivent être examinées et testées pour s'assurer qu'il n'y a pas d'impact négatif sur les opérations ou la sécurité de celui-ci.
	P4.2.4	Restrictions sur les modifications apportées aux progiciels
		Les modifications apportées aux progiciels seront déconseillées, limitées aux modifications nécessaires et toutes les modifications seront strictement contrôlées.
	P4.2.5	Principes d'ingénierie des systèmes sécurisés
		Les principes d'ingénierie des systèmes sécurisés doivent être établis, documentés, maintenus et appliqués à tout effort de mise en œuvre de systèmes d'information.
	P4.2.6	Environnement de développement sécurisé
		Les OSE doivent établir et protéger de manière appropriée des environnements de développement sécurisés lors des développements et d'intégration de systèmes qui couvrent l'ensemble du cycle de vie desdits systèmes.
	P4.2.7	Développement externalisé
		L'OSE doit superviser et surveiller l'activité de développement de systèmes externalisés.
	P4.2.8	Tests de sécurité du système
		Des essais de la fonctionnalité de sécurité doivent être effectués pendant le développement.
	P4.2.9	Tests d'acceptation du système

		Des programmes d'essais d'acceptation et des critères connexes doivent être établis pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions.

P4.3	Données à tester	
Objectif	Contrôle des données à des fins de test	
Contrôle	S'assurer que les données utilisées pour les tests sont sécurisées et n'exposent pas les OSE	
Sous-contrôles	P4.3.1	Protection des données d'essai
		Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées.

P4.4	Séparation des environnements de développement, de tests et de production	
Objectif	Dans le cadre de la mise en œuvre de nouvelles applications logicielles ou dans le cadre de modifications de logiciels existants, l'OSE sépare les environnements de développements, de tests, de production et les sécurise.	
Contrôle	Assurer la séparation de l'environnement de test, du développement et de la production	
Sous-contrôles	P4.4.1	Disposer des contrôles documentés du mouvement des données
		Définir les règles de transferts des logiciels du niveau de développement à celui de production.
	P4.4.2	Test des systèmes avant l'environnement de production
		Tests obligatoires des modifications des systèmes logiciels en production dans un environnement de tests séparé, avant leur mise en œuvre, avec documentation des mesures de sécurité complémentaires. Toute impossibilité technique ou organisationnelle à cet égard doit être documentée.
	P4.4.3	Accès du personnel pour tester l'environnement
		L'accès du personnel de développement et de tests à l'environnement de production est documenté, limité au minimum nécessaire et contrôlé.
	P4.4.4	Utilisation minimale des données en direct
		Dans les environnements de tests et de développement, les données réelles provenant de l'environnement de production (par exemple, les copies) doivent être limitées au minimum nécessaire.
	P4.4.5	Protection des données sensibles dans l'environnement de test
		Si des informations relatives à la sécurité de l'infrastructure essentielle sont disponibles dans les environnements de tests et de développement (par exemple données d'accès, détails de la

		configuration de sécurité), elles doivent être sécurisées de la même manière que dans l'environnement de production.
	P4.4.6	Suppression des données de test
		Si les environnements de tests et de développement ne sont pas (ou plus) utilisés, les données qui y sont recueillies doivent être supprimées en toute sécurité. Ce processus doit être documenté.
	P4.4.7	Protection des nouveaux logiciels
		Les procédures de mise en œuvre de nouvelles applications logicielles, de modifications des applications logicielles existantes au sein des IE doivent être décrites dans le PSO.
	P4.4.8	Cloisonnement
		Le réseau OSE sera logiquement et si possible physiquement séparé entre différentes fonctions telles que DNS et courrier, systèmes externes et internes ainsi que des tiers. Le trafic réseau sera contrôlé par des systèmes tels que des pares-feux et ne sera autorisé que lorsque les exigences de l'entreprise le justifient avec les autorisations appropriées. Le trafic autorisé doit être surveillé, sécurisé et documenté, une documentation précise à ce sujet doit être maintenue et tenue à jour.

P5 – Sécurité des opérations

Il est important de maintenir des opérations sécurisées dans l'ensemble des OSE afin de s'assurer que les activités opérationnelles n'exposent pas l'OSE aux menaces liées à la cybersécurité. Le domaine fournit des exigences pour la mise en œuvre des contrôles de sécurité, y compris les procédures connexes pour la conformité des OSE.

P5.1	Procédures opérationnelles et responsabilités	
Objectif	S'assurer que des procédures correctes sont en place et mises en œuvre	
Contrôle	Avoir des procédures opérationnelles documentées et mises en œuvre	
Sous-contrôles	P5.1.1	Procédures d'exploitation documentées
		Toutes les procédures opérationnelles doivent être documentées et mises en œuvre.
	P5.1.2	Gestion du changement
		Tous les changements doivent être documentés et contrôlés.
	P5	Gestion de la capacité
		Surveiller l'utilisation des ressources pour assurer une capacité adéquate pour l'avenir.

P5.2	Protection contre les logiciels malveillants	
Objectif	S'assurer que les informations et les installations de traitement de l'information sont protégées contre les logiciels malveillants	
Contrôle	Se protéger contre les logiciels malveillants	
Sous-contrôles	P5.2.1	Détecter et prévenir les logiciels malveillants
		Des contrôles de détection, de prévention et de récupération pour se protéger contre les logiciels malveillants doivent être mis en œuvre, combinés à une sensibilisation appropriée des utilisateurs.
	P5.2.2	Installation antivirus
		A propos des anti-virus : a. L'installation et l'assurance du bon fonctionnement et de la mise à jour systématique des anti-virus doit être assurée b. Les anti-virus vérifient, entre autres, avant le lancement d'un fichier, sa prévalence et sa signature numérique (par l'utilisation, par exemple, de logiciels antivirus basés sur l'heuristique et l'évaluation de la réputation).
	P5.2.3	Liste blanche des applications
		L'utilisation de logiciels de confiance, pour empêcher l'exécution de codes malveillants en bloquant les fichiers.exe, les DLL, les scripts (par exemple Windows Script Host, PowerShell et HTA) et les installateurs. A cette fin, il est nécessaire, autant que possible, d'utiliser les listes blanches d'applications autorisées.
	P5.2.4	Protection des systèmes industriels
		Les systèmes pour lesquels il n'est pas possible de mettre en œuvre les améliorations de sécurité recommandées (par exemple les systèmes d'OT[1]), d'autres mesures de sauvegarde assurant un niveau de sécurité adéquat sont prévues et mises en œuvre. [1]*OT ou Operational Technology (Technologie Opérationnelle en francais) désigne un système informatique dédié à l'environnement des systèmes de contrôle industriels (surveillance et/ou contrôle direct d'équipements, de biens, de processus et d'évènements industriels). L'OT présente des différences technologiques et fonctionnelles avec les systèmes informatiques traditionnels.*
	P5.2.5	Sécurisation des macros
		La configuration du support des macros Microsoft Office, afin de bloquer les macros des documents téléchargés sur Internet et pour n'autoriser que les macros testés et approuvés, entre autres des macros signées numériquement à partir d'une source fiable. Pour les autres macros, ne permettre leur exécution que dans un "environnement sécurisé" avec des droits d'écriture limités.
	P5.2.6	Utilisation d'un certificat électronique de confiance
		Les applications qui nécessitent Java sont exécutées après avoir été ajoutées à la liste des applications sûres ou utilisant des certificats électroniques fiables.

P5.3	Contrôle des logiciels opérationnels	
Objectif	Assurer l'intégrité des systèmes opérationnels.	
Contrôle	Avoir des procédures documentées d'installation de logiciels sur le système opérationnel	
Sous-contrôles	P5.3.1	Installation de logiciels sur les systèmes opérationnels
		Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciels sur les systèmes opérationnels.
	P5.3.2	Installation de la dernière version
		L'OSE installe les dernières versions du logiciel et du matériel, sauf si des exceptions sont obtenues et autorisées à installer une version inférieure à la version la plus récente. L'OSE applique les conditions suivantes : a. Préalablement à l'installation de toute nouvelle version, l'OSE : - S'assure de l'origine de cette version et de son intégrité ; - Analyse son impact technique et opérationnel sur l'IE. b. Dès qu'il a connaissance d'une nouvelle version ou d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'OSE en planifie l'installation après avoir effectué les vérifications mentionnées précédemment, et procède à cette installation dans les délais prévus par la procédure de surveillance et de mise à jour des conditions de sécurité des IE. c. Les systèmes d'exploitation ainsi que les équipements réseaux de l'OSE sont utilisés dans leur version légale actuelle et sont tenus à jour. d. Les versions de ressources matérielles ou logicielles non supportées ne sont pas utilisées, sauf par décision de l'OSE, lorsque des raisons techniques ou opérationnelles justifient, pour certaines ressources de ses IE, de ne pas installer la dernière version et/ou une version supportée par le fournisseur, l'éditeur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'OSE met en œuvre des mesures techniques ou organisationnelles prévues par la procédure de surveillance et de mise à jour des conditions de sécurité des IE pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues.

P5.4	Configuration	
Objectif	Garantir des configurations sécurisées de tous les systèmes OSE	
Contrôle	Avoir des pratiques de configuration sécurisées	
Sous-contrôles	P5.4.1	Installations restreintes
		L'OSE installe sur ses IE les seuls services et fonctionnalités qui sont indispensables à leur fonctionnement ou à leur sécurité. Il désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'OSE le mentionne dans le PSO en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre.
	P5.4.2	Contrôle des logiciels utilitaires
		Entre autres, l'OSE limite et supervise l'utilisation de logiciels utilitaires de contournement de la sécurité des systèmes et des applications. Les logiciels utilitaires peuvent être des programmes pour, par exemple, l'optimisation des systèmes, la virtualisation, ainsi que des interprètes de commandes tels que Windows PowerShell. Les logiciels utilitaires utilisés sont enregistrés ou soumis à des procédures d'identification, d'authentification et d'autorisation, et il est mis en œuvre une séparation de ces utilitaires des applications. L'OSE crée, maintient et surveille une liste de logiciels utilitaires approuvés, et supprime ou bloque l'utilisation de tous les programmes utilitaires inutiles.
	P5.4.3	Utilisation des supports amovibles
		L'OSE ne connecte à ses IE que des équipements, matériels périphériques et supports amovibles dont il assure la gestion et qui sont indispensables au fonctionnement ou à la sécurité de ses IE. Tout autre utilisation de support amovible est interdite.
	P5.4.4	Rechercher les logiciels malveillants avant d'utiliser le support amovible
		L'OSE procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de codes malveillants. L'OSE met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de codes malveillants provenant de ces supports.
	P5.4.5	Protection des appareils informatiques fonctionnant hors site
		L'OSE dispose de procédures et de mécanismes pour protéger ses propres appareils ou équipements mobiles hors sites. Les procédures doivent comprendre au moins : a) Des exigences relatives à la protection physique des équipements ; b) Des limitations d'installation de logiciels ; c) Des règles de protection contre les accès non autorisés ; d) Des règles d'utilisation des services et applications Internet ; e) Des règles de conduite en cas de perte ou de détérioration d'un appareil.
	P5.4.6	Protection de l'information dans les médias sortant de l'OSE

		L'OSE dispose de procédures pour le traitement des équipements de téléinformatiques retirés de l'exploitation courante. Notamment, les supports devant définitivement sortir de l'OSE (par exemple par la vente, le transfert ou après utilisation) doivent être illisibles, par écrasement des données, destruction des supports, ou toutes autres actions adéquates.
	P5.4.7	Mettre en place une procédure pour bloquer les médias non autorisés
		Les procédures doivent inclure le blocage des supports CD/DVD/USB non approuvés et le blocage des connexions aux téléphones, tablettes et appareils Bluetooth/Wi-Fi/3G/4G/5G non approuvés.
	P5.4.8	Contrôle de l'installation du logiciel en production
		L'OSE élabore, met en œuvre et décrit dans son PSO les procédures d'installation et de supervision des logiciels en environnement de production, qui doivent comprendre au moins : a) Les règles de mise à jour des logiciels en production, des applications et des bibliothèques ; b) Les règles d'admission des seuls codes exécutables acceptés et testés dans les systèmes en production (ne pas admettre les codes en compilation ou les codes en cours de développement) ; c) Les règles de restauration d'une version antérieure du système, y compris les comportements des versions antérieures des logiciels.

P5.5	Identité numérique	
Objectif	Protéger l'identité numérique de l'OSE	
Control	Mettre en place des certificats numériques de confiance	
Sub-Controls	P5.5.1	Mise en œuvre du certificat numérique approuvé
		Afin de garantir l'identité numérique de l'OSE, la fiabilité des services proposés et la confidentialité et l'intégrité des transactions, tous les sites web ou applications essentielles mis à dispositions des utilisateurs par l'OSE doivent être protégés par un certificat électronique émis par une autorité de certification approuvée par l'entité togolaise compétente.

P6 – Sécurité environnementale et physique

Protéger les actifs de l'environnement contre l'accès non autorisé et l'utilisation abusive des installations physiques abritant et traitant l'infrastructure numérique.

P6.1	Accès physique
Objectif	Empêcher l'accès physique non autorisé, les dommages et les interférences aux installations de traitement de l'information de l'OSE.
Contrôle	Mettre en place des contrôles physiques pour empêcher l'accès non autorisé aux locaux d'OSE, en particulier si ces lieux stockent et traitent des informations sensibles.

Sous-contrôles	P6.1.1	Périmètre de sécurité physique
		Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones qui contiennent des informations sensibles ou critiques et les installations de traitement de l'information.
	P6.1.2	Contrôles d'entrée physiques
		Les zones sécurisées doivent être protégées par des contrôles d'entrée appropriés pour s'assurer que seul le personnel autorisé est autorisé à y accéder.
	P6.1.3	Sécurisation des bureaux, des chambres et des installations
		La sécurité physique des bureaux, des locaux et des installations doit être conçue et appliquée.
	P6.1.4	Protection contre les menaces extérieures et environnementales
		Une protection physique contre les catastrophes naturelles, les attaques malveillantes ou les accidents doit être conçue et appliquée.
	P6.1.5	Travailler dans des zones sécurisées
		Les procédures de travail dans des zones sécurisées doivent être conçues et appliquées.
	P6.1.6	Zone de livraison et de chargement
		Les points d'accès tels que les zones de livraison et de chargement et les autres points où des personnes non autorisées pourraient entrer dans les locaux doivent être contrôlés et, si possible, isolés des installations de traitement de l'information afin d'éviter tout accès non autorisé.

P6.2	**Équipements**	
Objectif	Prévenir la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des opérations de l'OSE	
Contrôle	Mettre en place des processus et des mécanismes pour protéger les équipements en tout temps.	
Sous-contrôles	P6.2.1	Emplacement et protection de l'équipement
		L'équipement doit être placé et protégé de manière à réduire les risques liés aux menaces et aux dangers environnementaux ainsi que les possibilités d'accès non autorisé.
	P6.2.2	Protection contre les pannes électriques
		L'équipement doit être protégé contre les pannes de courant et autres perturbations causées par des défaillances électriques.
	P6.2.3	Sécurité du câblage
		Les câbles d'alimentation et de télécommunications transportant des données ou soutenant des services d'information sont protégés contre l'interception, les interférences ou les dommages.
	P6.2.4	Entretien de l'équipement
		L'équipement doit être correctement entretenu pour assurer sa disponibilité et son intégrité continues.
	P6.2.5	Décommissionnement des actifs
		L'équipement, l'information ou le logiciel ne doivent pas être retirés du site sans autorisation préalable.
	P6.2.6	Sécurité de l'équipement et des biens hors site

		La sécurité doit être appliquée aux biens hors site en tenant compte des différents risques liés au travail à l'extérieur des locaux de l'OSE.
	P6.2.7	Elimination ou réutilisation sécuritaires de l'équipement
		Tous les équipements contenant des supports de stockage doivent être vérifiés pour s'assurer que toutes les données sensibles et les logiciels sous licence ont été supprimés ou écrasés en toute sécurité avant d'être éliminés ou réutilisés.
	P6.2.8	Equipement utilisateur sans surveillance
		Les utilisateurs doivent s'assurer que les équipements sans surveillance bénéficient d'une protection appropriée.
	P6.2.9	Nettoyer les bureaux et les écrans
		Une politique de bureau propre limitant les papiers et les supports de stockage amovibles et une politique d'écran propre doivent être adoptées.

D1 – Gestion des incidents de sécurité

La défense des réseaux et systèmes d'information consiste en une veille active de la sécurité informatique des Opérateurs de Services Essentiels et de leurs Infrastructures Essentielles. Pour la défense de ses réseaux et systèmes d'information, l'OSE élabore et met en œuvre un service spécialisé de surveillance, de détection, d'analyse et de qualification des évènements de sécurité, appelé service de Security Operations Center (SOC).

D1.1	Journalisation et surveillance	
Objectif	Enregistrer les événements et générer des preuves	
Contrôle	Consigner et surveiller les événements de sécurité	
Sous-contrôles	D1.1.1	Journalisation des événements
		Des journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défauts et les événements de sécurité de l'information doivent être produits, conservés et régulièrement examinés.
	D1.1.2	Protection des informations de journal
		Les activités de l'administrateur de réseau et du gestionnaire de réseau sont consignées et les journaux protégés et régulièrement révisés.
	D1.1.3	Synchronisation de l'horloge
		Les horloges de tous les systèmes de traitement de l'information pertinents au sein d'un OSE ou d'un domaine de sécurité doivent être synchronisées avec une source de temps de référence unique.

D1.2	Surveillance de la sécurité	
Objectif	Gérer les incidents de cybersécurité	
Contrôle	Assurer une approche cohérente et efficace de la gestion des incidents de sécurité	
Sous-contrôles	D1.2.1	Responsabilités et procédures
		Les responsabilités et les procédures de gestion doivent être établies pour assurer une réponse rapide, efficace et ordonnée aux incidents de sécurité de l'information.
	D1.2.2	Signalement des événements de cybersécurité
		Les événements liés à la sécurité de l'information doivent être signalés le plus rapidement possible par les canaux de gestion appropriés.
	D1.2.3	Signaler les faiblesses en matière de cybersécurité
		Les employés et les sous-traitants qui utilisent les systèmes et services d'information de l'OSE sont tenus de noter et de signaler toute faiblesse observée ou soupçonnée en matière de sécurité de l'information dans les systèmes ou les services.
	D1.2.4	Evaluation et décision sur les événements de sécurité de l'information

		Les événements liés à la sécurité de l'information sont évalués et il est décidé s'ils doivent être classés comme incidents de sécurité de l'information.
	D1.2.5	Réponse aux incidents de cybersécurité
		Les incidents de sécurité de l'information doivent être traités conformément aux procédures documentées.
	D1.2.6	Apprendre des incidents de cybersécurité
		Les connaissances acquises grâce à l'analyse et à la résolution des incidents de sécurité de l'information doivent être utilisées pour réduire la probabilité ou l'impact d'incidents futurs.
	D1.2.7	Collecte de preuves
		L'organisme doit définir et appliquer des procédures pour l'identification, la collecte, l'acquisition et la conservation de renseignements qui peuvent servir de preuve.

D1.3	Surveillance des incidents de cybersécurité	
Objectif	Surveiller les incidents de cybersécurité 24 heures sur 24, 7 jours sur 7	
Contrôle	Mettre en place des fonctions et des outils appropriés pour la surveillance des événements de sécurité en permanence	
Sous-contrôles	D1.3.1	Avoir un système de détection des incidents de sécurité
		L'OSE met en œuvre les dispositifs de détection capables d'identifier des événements caractéristiques d'un incident de sécurité notamment d'une attaque en cours ou à venir et de permettre la recherche de traces d'incidents antérieurs. A cet effet, ces dispositifs : a. Collectent les données pertinentes sur le fonctionnement de chaque IE (notamment les données « réseau » et les données « système ») à partir de capteurs positionnés de manière à identifier les événements de sécurité liés à l'ensemble des flux de données échangés entre les IE et les systèmes d'information tiers à ceux de l'OSE. b. Analysent les données issues des capteurs notamment en recherchant des indicateurs de compromission, dans le but d'identifier les événements de sécurité et de les caractériser. c. Archivent les métadonnées des événements identifiés afin de permettre une recherche a posteriori de marqueurs techniques d'attaques ou de compromission sur une durée d'au moins six (6) mois. L'OSE veille en particulier à ce que l'installation et l'exploitation des dispositifs de détection n'affectent pas la sécurité et le fonctionnement de ses IE.
	D1.3.2	Journalisation des événements
		L'OSE met en œuvre pour chaque Infrastructure Essentielle un système de journalisation, de corrélation et d'analyse, opérationnel 24h/24 et 7j/7 tous les jours de l'année, dédié exclusivement à des fins de détection d'évènements de sécurité, qui enregistre les

		événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité de l'IE ainsi qu'au fonctionnement de l'IE.
	D1.3.3	Systèmes pour générer des journaux
		Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés précédemment : a. Les serveurs applicatifs des IE ; b. Les serveurs d'infrastructure système ; c. Les serveurs d'infrastructure réseau ; d. Les équipements de sécurité ; e. Les postes d'ingénierie et de maintenance des systèmes industriels ; f. Les équipements réseau ; g. Les postes d'administration ; h. Les postes utilisateurs (dans la mesure du possible).
	D1.3.4	Contenu des journaux d'événements
		Le journal des événements doit contenir au minimum des informations sur : a. L'identifiant de chaque utilisateur ; b. La date, l'heure et les détails des événements importants, tels que le début et la fin du travail dans le système, y compris les tentatives de connexion infructueuses ; c. Les modifications de la configuration du système ; d. L'utilisation de privilèges ; e. Les modifications de privilèges ; f. L'utilisation d'utilitaires et d'applications système sélectionnés ; g. Les adresses réseau ; h. Les alarmes déclenchées par le système de contrôle d'accès ; i. L'activation et la désactivation des systèmes de protection tels que les logiciels antivirus.
	D1.3.5	Protection de l'intégrité des journaux
		Aucun droit de suppression ou de désactivation des journaux contenant des enregistrements de leurs propres actions ne doit être attribué aux administrateurs de systèmes informatiques. Concernant les systèmes pour lesquels ce n'est pas possible, un mécanisme de copie vers un dépôt externe doit être mis en place.
	D1.3.6	Horodatage des journaux d'événements
		Les événements enregistrés par le système de journalisation sont horodatés. Ils sont centralisés et archivés pendant une durée d'au moins six (6) mois. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.
	D1.3.7	Maintenir à jour l'état de surveillance
		L'OSE élabore et met en œuvre une procédure de veille, de surveillance, d'obtention et de mise en œuvre des informations les plus récentes concernant, les vulnérabilités, les menaces techniques et les mesures correctrices de sécurité concernant les ressources matérielles et logicielles utilisées pour les Infrastructures Essentielles.

D1.4	Gestion des vulnérabilités techniques	
Objectif	Prévenir l'exploitation des vulnérabilités techniques	
Contrôle	Identifier et gérer les vulnérabilités	
Sous-contrôles	D1.4.1	Gestion des vulnérabilités techniques
		Les informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues en temps utile. L'exposition de l'OSE à ces vulnérabilités est évaluée et les mesures appropriées prises pour faire face au risque associé des vulnérabilités sont identifiées.
	D1.4.2	Restrictions sur l'installation du logiciel
		Les règles régissant l'installation des logiciels par les utilisateurs sont établies et mises en œuvre.
	D1.4.3	Notation des vulnérabilités
		Les vulnérabilités identifiées sont notées sur la base de normes de notation communes de l'industrie. L'OSE élabore un plan d'action de remédiation fondé sur la notation de la vulnérabilité.
	D1.4.4	Vulnérabilités liées à Internet
		L'OSE identifie régulièrement toutes les vulnérabilités liées à l'internet au moins une fois par mois et corrige les vulnérabilités identifiées dans les deux semaines suivant leur identification.

ANCy Agence Nationale de la Cybersécurité

R1 – Gestion de la continuité des activités

Ce domaine identifie les exigences pour les OSE afin de construire et d'exploiter des services essentiels durables contre des événements désastreux imprévus tels que des incendies, des inondations, des troubles politiques, etc.

R1.1	Sauvegarde	
Objectif	Se protéger contre la perte de données	
Contrôle	Réaliser la sauvegarde des informations	
Sous-contrôles	R1.1.1	Test des sauvegardes
		Des copies de sauvegarde des informations, des logiciels et des images système doivent être prises et testées régulièrement conformément à une politique de sauvegarde convenue.

R1.2	Continuité des opérations commerciales	
Objectif	Construire des services résilients et s'assurer que les OSE peuvent supporter des événements désastreux susceptibles d'avoir un impact sur les services et les opérations essentiels	
Contrôle	Avoir des opérations essentielles résilientes en cas d'événement désastreux impardonnable	
Sous-contrôles	R1.2.1	Politique de gestion de la continuité des activités
		Maintenir une politique de gestion de la continuité des activités couvrant la continuité et la redondance des informations en fonction de leur niveau de criticité.
	R1.2.2	Plan de continuité des activités
		Mettre en place un plan de continuité des activités de l'OSE et qui décrit ce qu'il faut faire en cas d'événement désastreux imprévu.
	R1.2.3	BIA (Business Impact Assessment)
		Effectuer une évaluation de l'impact sur l'entreprise pour tous les processus opérationnels et systèmes d'information critiques.

R1.3	Aspect cybersécurité de la continuité des activités	
Objectif	Disposer de contrôles et de services de cybersécurité résilients pour les OSE	
Contrôle	Avoir des opérations de cybersécurité résilientes en cas d'événement désastreux critiques tels que la corruption des données, l'indisponibilité du système critique.	
Sous-contrôles	R1.3.1	Planification de la continuité de la cybersécurité
		L'OSE doit déterminer ses exigences en matière de sécurité de l'information et de continuité de la gestion de la sécurité de l'information dans des situations défavorables, par exemple lors d'une crise ou d'une catastrophe.
	R1.3.2	Mise en œuvre de la continuité de la cybersécurité
		L'OSE doit établir, documenter, mettre en œuvre et maintenir des processus, des procédures et des contrôles afin d'assurer le niveau

		requis de continuité pour la sécurité de l'information dans une situation défavorable.
	R1.3.3	Vérifier, examiner et évaluer la continuité de la sécurité de l'information
		L'organisme doit vérifier les contrôles de continuité de la sécurité de l'information établis et mis en œuvre à intervalles réguliers afin de s'assurer qu'ils sont valides et efficaces dans des situations défavorables.

R1.4	Test de la capacité de continuité des activités	
Objectif	Avoir un processus de tests réguliers pour assurer la préparation en cas de catastrophe	
Contrôle	Avoir des plans de tests et effectuer des tests réguliers	
Sous-contrôles	R1.4.1	Elaborer un plan d'essai
		Développer des plans de tests complets pour toutes les opérations critiques simulant divers scénarios de catastrophe, y compris, sans s'y limiter, les inondations, les cyberattaques, les ransomwares, les incendies, etc.
	R1.4.2	Effectuer des tests réguliers
		Les tests doivent être effectués régulièrement au moins deux fois par an avec une période de quatre à six mois entre chaque test.

R1.5	Gestion de crise	
Objectif	Mettre en place un processus de gestion de crise pour répondre efficacement à un événement indésirable	
Contrôle	Élaborer des plans et une structure de gestion de crise	
Sous-contrôles	R1.5.1	Elaborer un processus et une procédure de gestion de crise
		Les OSE doivent disposer d'un processus et d'une procédure de gestion de crise pour répondre à un événement indésirable.
	R1.5.2	Construire une structure de gestion de crise
		L'OSE doit avoir une structure de gestion de crise en place comprenant la haute direction et couvrant toutes les ressources requises.

R1.6	Reprise après sinistre	
Objectif	Mettre en place un processus pour se remettre efficacement d'un événement indésirable	
Contrôle	Construire des processus et des systèmes redondants pour assurer la continuité des services	
Sous-contrôles	R1.6.1	Disponibilité des installations redondantes critiques

		Les OSE auront tous les services critiques identifiés pour disposer d'une infrastructure redondante afin d'assurer une prise de contrôle en douceur en cas d'événements indésirables.
	R1.6.2	Processus et procédures de récupération documentés
		Les OSE doivent avoir des processus et des procédures de rétablissement documentés alignés sur la politique globale de gestion de la continuité des activités

6. Références

L'élaboration de ces règles est fondée sur les normes de l'industrie et les pratiques exemplaires communes en matière de protection nationale de la cybersécurité, qui sont, mais sans s'y limiter :

1. ISO 27001:2013 - Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
2. PCI DSS (normes de sécurité des données pour l'industrie des cartes de paiement)
3. NIST 800-53 Révision 5 « Contrôles de sécurité et de confidentialité pour les systèmes d'information fédéraux et les organisations »
4. The 18 CIS Critical Security Controls
5. SANS Critical Security Controls (SANs Top 20)

7. Facteurs clés de succès

La mise en œuvre des règles détaillées de cybersécurité mentionnées dans le présent document dans l'ensemble des quatorze domaines devrait être caractérisée par les résultats ci-dessous :

1. Réduction significative du nombre d'incidents de sécurité mesurés sur une période de temps dans l'ensemble de l'OSE
2. Augmentation du niveau de sensibilisation aux cybermenaces pour tous les employés de l'OSE, mesurée par la diminution du nombre d'incidents de sécurité liés aux employés ainsi que par les résultats de scénarios d'attaque simulés.
3. Mener une sensibilisation, une formation et une éducation appropriées concernant ces règles de cybersécurité et des formations facilitées par l'industrie sur la cybersécurité pour tout le personnel de l'OSE
4. Existence d'un soutien et d'une implication visibles de la part des membres supérieurs de la direction de l'OSE pour défendre le cours de cybersécurité à l'OSE
5. L'OSE participe et contribue à l'industrie, au secteur et au partage à l'échelle nationale des meilleures pratiques en matière d'assurance de l'information et des leçons apprises avec l'ANCy et tout autre organisme de réglementation applicable.
6. Un budget indicatif prévoit toutes les activités de cybersécurité sur une base annuelle afin d'assurer des améliorations continues et la conformité.
7. L'OSE a une bonne compréhension et appréciation de la façon de mettre en œuvre les règles de cybersécurité en plus de la façon dont l'efficacité sera mesurée par ANCY et de mener une auto-évaluation
8. L'OSE a une voie d'escalade claire sur les incidents de sécurité critiques et sait comment et où demander de l'aide ainsi que signaler de tels incidents aux régulateurs et aux autorités.
9. Avoir un PSO clair et régulièrement mise à jour avec une ventilation détaillée des mesures que l'OSE entreprendra pour répondre aux exigences de conformité
10. Avoir des rapports d'évaluation des risques à jour détaillant la méthodologie utilisée et les détails des risques identifiés et des plans d'assainissement documentés.

ARRETE N° 0228/MATDDT-CAB DU 14/06/2022 portant autorisation d'installation sur le territoire togolais de l'Organisation Etrangère dénommée : «DEUTSCHER VOLKSHOCHSCHUL-VERBAND E.V» (D.V.V)

LE MINISTRE D'ETAT, MINISTRE DE L'ADMINISTRATION TERRITORIALE, DE LA DECENTRALISATION ET DU DEVELOPPEMENT DES TERRITOIRES

Vu la loi n° 40-484 du 1er Juillet 1901 relative au contrat d'association ;

Vu le décret n° 2022-002/PR du 05 janvier 2022 fixant les conditions de coopération entre les Organisations Non - Gouvernementales (ONG) et le Gouvernement ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'État et ministres ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du Gouvernement, ensemble les textes qui l'ont modifié ;

Vu la demande d'autorisation d'installation en date du 20 janvier 2021 introduite par **Madame AHADJI M. Sophie** 1re Représentante de ladite Organisation au Togo ;

Vu la lettre du 07 juin 2022 notifiant la nomination de **Monsieur OURO OKOUROU Wakilou** comme nouveau représentant de l'organisation au Togo.

Vu les conclusions du rapport d'enquête n° 877/4 de la Brigade Territoriale de la Gendarmerie nationale d'Agoè-Nyivé du 28 août 2021 sur ladite organisation ;

ARRETE :

Article premier : Il est accordé à l'Organisation étrangère dénommée « **DEUTSCHER VOLKSHOCHSCHUL-VERBAND E.V** » **(D.V.V.)** inscrite au registre des associations du Tribunal d'Instance de BONN le 19 juillet 2005 sous le numéro VR 3120 et dont le siège se trouve à BONN en Allemagne, l'autorisation de s'installer sur le territoire togolais avec pour objectif d'appuyer les structures sociales à pouvoir améliorer leurs actions à travers l'éducation et la formation continue.

Art. 2 : Conformément à l'objet de l'Organisation, un accord-programme arrêté par le Ministère de la Planification du Développement et de la Coopération complétera les présentes dispositions.

Art. 3 : Le présent arrêté qui prend effet à compter de la date de sa signature sera publié au Journal Officiel de la République Togolaise.

Fait à Lomé, le 14 juin 2022

Le ministre de L'Administration Territoriale, de La Décentralisation et du Développement des Territoires

Payadowa BOUKPESSI

ARRETE N° 003/MENTD/CAB DU 12/07/2022 fixant les conditions de mise en œuvre de l'itinérance nationale

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par le décret n° 2018-145/PR du 3 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 ;

Vu le décret n° 2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de régulation des communications électroniques et des postes ;

Vu le décret n° 2018-174/PR du 10 décembre 2018 fixant les taux, les modalités de recouvrement et d'affectation des redevances dues par les opérateurs et exploitants de réseaux et services de communications électroniques, les fournisseurs d'équipements et terminaux et les installateurs d'équipements radioélectriques ;

Vu le décret n° 2018-070/PR du 18 avril 2018 relatif au service universel des communications électroniques ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du gouvernement complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu l'arrêté n° 005/MENTD/CAB du 29 avril 2021 portant définition des indicateurs de qualité des services mobiles 2G, 3G. 4G et de leurs seuils ;

Vu l'arrêté n° 005/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l'opérateur Togo Cellulaire pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles ;

Vu l'arrêté n° 006/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l' opérateur Atlantique Telecom Togo pour l'établissement et l'exploitation de réseaux de réseaux de communications électroniques mobiles ;

Vu le cahier des charges de l'opérateur Atlantique Telecom Togo du 18 décembre 2018 pour l'établissement et l'exploitation de réseaux de

communications électroniques mobiles 2G, 3G et 4G ;

Vu le cahier des charges de l'opérateur Togo Cellulaire du 22 novembre 2019 pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles 2G, 3G et 4G ;

ARRETE :

CHAPITRE 1ER : DISPOSITIONS GENERALES

Article premier : Objet

Le présent arrêté pris en application de l'article 28 de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013 (ci-après la « **LCE** ») et de l'article 31.3 du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 (ci-après le « **Décret interconnexion** »), a pour objet de préciser les conditions et les modalités de mise en œuvre de l'itinérance nationale.

Art. 2 : Définitions

Les termes utilisés dans le présent arrêté ont la signification que leur confèrent la LCE et le Décret interconnexion.

CHAPITRE II : REGLES GENERALES APPLICABLES A L'ITINERANCE NATIONALE

Art. 3 : Traitement des demandes d'itinérance nationale

L'opérateur désirant recourir à l'itinérance nationale en fait la demande par écrit à l'opérateur concerné. Une copie de la demande écrite est transmise pour information à l'Autorité de régulation conformément aux dispositions 5.1 et 5.2 du Décret interconnexion.

Le demandeur fournit les caractéristiques de l'accès demandé, notamment :

(i) les zones précises du territoire concernées par la demande ;
(ii) les éléments du réseau en question ;
(iii) les capacités requises et les modalités d'exploitation proposées ;
(iv) les interfaces d'accès du réseau concerné ;
(v) la date de mise en œuvre demandée.

L'opérateur qui reçoit la demande fera droit dans les conditions prévues aux articles 5.4 à 5.8 du Décret interconnexion.

L'itinérance nationale ne peut être refusée que pour des motifs techniques et financiers suffisamment justifiés et motivés. Lorsque la demande d'itinérance nationale résulte d'une obligation de l'Autorité de régulation conformément à l'article 7 du présent arrêté, elle ne peut être refusée que pour des motifs de faisabilité techniques motivés.

En cas de refus de l'itinérance nationale, une copie de la lettre motivant le refus est adressée à l'Autorité de régulation conformément à l'article 5.7 du Décret d'interconnexion.

En cas de réponse favorable, les parties négocient et concluent, dans les trois (3) mois qui suivent la réception de la demande, une convention d'itinérance dans les conditions prévues à l'article 5.8 du Décret d'interconnexion.

Art. 4 : Conventions d'itinérance nationale

La prestation d'itinérance nationale fait l'objet d'un accord précisant notamment les conditions juridiques, techniques, opérationnelles et tarifaires figurant dans la convention d'itinérance nationale et respecte les principes d'objectivité, de transparence et de non-discrimination. Elles ne conduisent pas à imposer indûment des contraintes ou des charges excessives aux opérateurs utilisant l'itinérance nationale et sont susceptibles d'être justifiées sur demande de l'Autorité de régulation.

Les conventions d'itinérance conclues entre opérateurs sont obligatoirement communiquées à l'Autorité de régulation dans un délai de huit (8) jours à compter de leur signature. L'Autorité de régulation procède à l'examen des conventions d'itinérance nationale dans les conditions prévues à l'article 7.2 à 7.6 du Décret interconnexion.

L'Autorité de régulation peut demander aux parties à une convention d'itinérance nationale la modification des accords d'itinérance nationale déjà conclus afin de garantir l'égalité des conditions de concurrence entre les opérateurs dans les conditions prévues aux articles 7.4 et 7.5 du Décret interconnexion.

La convention d'itinérance nationale doit respecter le contenu minimal prévu à l'article 11 du Décret interconnexion.

Les exigences prévues à l'article 13 du Décret interconnexion sont applicables aux opérateurs qui concluent une convention d'itinérance nationale.

Les tarifs d'itinérance nationale sont inscrits dans le catalogue d'interconnexion dans les conditions prévues aux articles 15 et 16 du Décret interconnexion.

Art. 5 : Action de l'Autorité de régulation

Les dispositions de l'article 10 du Décret interconnexion s'appliquent en cas de refus, d'échec des négociations commerciales ou de désaccord sur la conclusion ou l'exécution d'une convention d'itinérance nationale.

Art. 6 : Confidentialité

Les parties à une convention d'itinérance nationale sont tenues au respect du principe de confidentialité prévu à l'article 12 du Décret interconnexion.

CHAPITRE III : REGLES SPECIFIQUES APPLICABLES A L'ITINERANCE NATIONALE

Art. 7 : Itinérance nationale pour des besoins de concurrence et d'aménagement du territoire

Lorsque l'itinérance nationale est nécessaire pour satisfaire aux objectifs de concurrence et de l'aménagement du territoire, l'Autorité de régulation peut en faire une obligation à la charge des opérateurs en publiant une liste des zones géographiques éligibles concernées par cette obligation et les conditions y afférentes. Dans les zones couvertes par cette liste, le déploiement et l'extension de la couverture des réseaux de communications électroniques sont réalisés par le recours prioritaire à des accords d'itinérance dans les conditions prévues par le présent article.

La liste des zones est révisée chaque année par l'Autorité de régulation afin d'adapter les périmètres des zones dans lesquelles des obligations d'itinérance sont imposées aux opérateurs en vue de répondre aux objectifs de concurrence et d'aménagement du territoire. En cas de modification substantielle de l'environnement technique, économique, règlementaire ou concurrentiel, l'Autorité de régulation pourra modifier exceptionnellement la liste des zones visées à l'alinéa 1 er du présent article.

Conformément à l'article 31.1 du Décret interconnexion, les opérateurs de réseaux de communications électroniques peuvent recourir à l'itinérance nationale, y compris pour remplir leurs obligations de couverture dans les conditions prévues dans leur cahier des charges.

Sans préjudice des obligations de déploiement mises à la charge des opérateurs de réseaux de communications électroniques dans leurs cahiers des charges, les opérateurs gardent la faculté de recourir à l'itinérance nationale pour la couverture des autres zones ne figurant pas dans la liste susvisée à l'alinéa 1er du présent article.

Dans les zones listées précitées à l'alinéa 1er du présent article, la mise en place de l'itinérance nationale se fera dans les conditions prévues aux articles 3 à 6 du présent arrêté.

Art. 8 : Schéma de déploiement

Dans les zones visées à l'alinéa 1er de l'article 7 du présent arrêté, chaque opérateur établit un schéma de déploiement prévisionnel pour les douze (12) mois à venir à compter de la date prévue dans la décision de l'Autorité de régulation concernant la liste des zones visées à l'alinéa 1er de l'article 7 du présent arrêté.

Chaque opérateur précise dans son schéma de déploiement prévisionnel notamment :

- les projets d'implantation de sites en indiquant notamment :

i. la zone exacte d'implantation des sites identifiés sur une carte selon un format fixé par l'Autorité de régulation ;
ii. les zones de couverture prévisionnelles des stations de base, identifiées sur une carte selon un format fixé par l'Autorité de régulation ;
iii. la nature exacte des services mobiles fournis par ces sites.

- les modifications de ses sites pour la fourniture de services mobiles différents, y compris, la nature des travaux à réaliser et les équipements qui y seront installés ;

- les sites pour lesquels des conventions d'itinérance sont déjà conclues.

Une décision de l'Autorité de régulation complétera le détail du contenu des schémas de déploiement prévisionnel prévues aux alinéas 1 et 2 du présent article.

Ce schéma de déploiement prévisionnel doit être communiqué à l'Autorité de régulation à la date prévue dans la décision visée à l'alinéa 3 du présent article.

Chaque opérateur transmet à l'Autorité de régulation à la date prévue dans la décision visée à l'alinéa 3 du présent article, les déploiements et modifications de sites effectués dans les zones visées à l'alinéa 1er de l'article 7 du présent arrêté. Ces informations figureront dans leur catalogue d'interconnexion dans les conditions prévues dans le Décret interconnexion.

Dans les zones visées à l'alinéa 1er de l'article 7, l'Autorité de régulation veille à la coordination de schémas de déploiement prévisionnel des opérateurs visées à l'alinéa 1er du présent article afin d'assurer le respect des objectifs de concurrence et d'aménagement du territoire.

Lorsque le schéma de déploiement prévisionnel d'un opérateur prévoit de couvrir une zone déjà couverte par une infrastructure existante d'un autre opérateur pour la fourniture de services similaires, l'Autorité de régulation invite l'opérateur concerné à conclure une convention d'itinérance nationale avec l'opérateur détenteur des infrastructures existantes. Dans ce cas, l'accord devra être conclu dans les conditions prévues à l'alinéa 5 de l'article 7 du présent arrêté.

Lorsque plusieurs opérateurs prévoient de couvrir dans leurs schémas de déploiement prévisionnel une même zone, l'Autorité de régulation invite les opérateurs concernés à s'entendre. A défaut d'accord, l'Autorité de régulation sera saisie pour trancher.

Art. 9 : Nouvel Entrant

Sans préjudice des obligations de déploiement contenues dans son cahier des charges pour la fourniture de services de communications électroniques après l'adoption du présent arrêté, tout opérateur nouvel entrant garde la faculté de recourir à l'itinérance nationale pour la couverture des autres zones ne figurant pas dans la liste visée à l'article 7 alinéa 1er du présent arrêté.

Les opérateurs sont tenus de faire droit aux demandes d'itinérance de l'opérateur nouvel entrant dans les conditions objectives, transparentes et non-discriminatoires et dans les conditions prévues aux articles 3 à 6 du présent arrêté pendant une période maximale après l'entrée en vigueur de leur licence qui sera déterminée par arrêté portant octroi de licence.

Art. 10 : Sites déployés dans le cadre du service universel

L'opérateur déployant des sites financés par le fonds du service universel prévu à l'article 18 de la LCE, fait obligatoirement droit à toute demande d'itinérance nationale présentée pour ces sites par d'autres opérateurs dans des conditions Objectives, transparentes et non- discriminatoires et dans les conditions prévues aux articles 3 à 6 du présent arrêté.

CHAPITRE IV : DISPOSITIONS DIVERSES ET FINALES

Art. 11 : Règlement des différends

En cas de refus d'une demande d'itinérance ou en cas d'échec des négociations, ou s'il existe un désaccord sur l'exécution de l'accord d'itinérance nationale, l'Autorité de régulation pourra être saisie, le cas échéant, en règlement de différend dans les conditions prévues aux articles 29 et 30 de la LCE.

Art. 12 : Entrée en vigueur et publication

Le présent arrêté entre en vigueur à compter de la date de sa signature et sera publié au Journal Officiel de la République Togolaise.

Art. 13 : Exécution

Le directeur général de l'Autorité de régulation des communications électroniques et des postes est chargé de l'exécution du présent arrêté.

Fait à Lomé, le 12 juillet 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

ARRETE N° 005/MENTD/CAB DU 12/08/2022 portant définition des indicateurs de qualité des services mobiles 2G, 3G, 4G et leurs seuils

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'Etat et ministres ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié le décret n° 2018-145/PR du 03 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 03 octobre 2018 ;

Vu le décret n° 2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu le décret n° 2020-023/PR du 07 avril 2020 portant nomination des membres du Comité de Direction de l'Autorité de. Régulation des Communications Electroniques et de Postes (ARCEP) et de son président ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du gouvernement complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu le décret n° 2020-085/PR du 15 octobre 2020 portant nomination du directeur général de l'Autorité de régulation des communications électroniques et des postes (ARCEP) ;

Vu le décret n° 2021-073/PR du 24 Juin 2021 portant procédure de règlement de différends, de conciliation et de sanction devant l'Autorité de régulation des communications électroniques et des postes ;

Vu l'arrêté n° 005/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l'opérateur Togo Cellulaire pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles ;

Vu l'arrêté n° 006/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l'opérateur Atlantique Telecom Togo pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles ;

Vu le cahier des charges de l'opérateur Atlantique Telecom Togo du 18 novembre 2018 pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles 2G, 3G et 4G ;

Vu le cahier des charges de l'opérateur Togo Cellulaire du 22 novembre 2019 pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles 2G, 3G et 4G ;

ARRETE :

Article premier : Objet

Le présent arrêté détermine les indicateurs de qualité des services de communications électroniques mobiles 2G, 3G et 4G et définit les seuils à atteindre par les exploitants de réseaux mobiles ouverts au public.

Ces indicateurs et seuils sont décrits dans l'annexe 1 du présent arrêté.

Art. 2 : Champ d'application

Le présent arrêté s'applique à tous les opérateurs de réseaux de communications électroniques mobiles ouverts au public conformément au déploiement de leurs réseaux.

Art. 3 : Définitions

Aux termes du présent arrêté, on entend par :

1. Débit de transmission des données : Volume de données (en bits, kbits ou Mbits) écoulé par unité de temps au niveau de la couche application (FTP, http, etc.) pour un nombre de sessions dans le sens montant (Uplink) ou dans le sens descendant (Downlink).

2. Disponibilité d'une station de base : Aptitude d'une station de base à rendre possible l'accès au réseau sur un espace géographique appelé cellule, calculée par heure, par jour, par mois ou par an.

3. Drive test : Mesure de la couverture et de la qualité de services des réseaux mobiles au moyen d'une chaine de mesure embarquée dans un véhicule.

4. FTP : en anglais File Transfer protocol est le protocole de transfert de fichier utilisé pour télécharger ou charger des fichiers.

5. HTTP: en anglais HyperText Transfer Protocol est le protocole de transmission permettant à l'utilisateur d'afficher des pages Internet par l'intermédiaire d'un navigateur.

6. Localité : Ville, village ou quartier de ville tel que contenu dans la base de données de l'Institut National de la statistique et des études économiques et démographiques.

7. MOS : en anglais Mean Opinion Score est la note moyenne d'appréciation de la qualité d'écoute des appels téléphoniques.

8. OMC-R : en anglais Operation and Maintenance Center - Radio est un élément de base d'un réseau de téléphonie mobile chargé d'assurer la gestion des stations de base et de produire des statistiques relatives à l'activité du réseau.

9. QoE : en anglais Quality of Experience est l'acceptabilité globale d'une application ou d'un service, telle qu'elle est perçue subjectivement par l'utilisateur final. La qualité de l'expérience comprend l'ensemble des effets du système de bout en bout (client, terminal, réseau, infrastructure de services, etc.) et l'acceptabilité globale peut être influencée par les attentes des utilisateurs et le contexte.

10.QoS : en anglais Quality of Service ou qualité de service en français est la capacité d'un réseau à respecter les exigences de fourniture d'un type de service de communications électroniques notamment en termes d'accessibilité, de disponibilité, de continuité et d'intégrité.

11. Qualité MOS : Qualité de la communication (audio ou vidéo) mesurée selon le principe de calcul de la MOS. On distingue quatre niveaux de qualité :

• Qualité parfaite : si la moyenne des notes MOS attribuées est supérieure ou égale à 4 (MOS e™ 4) ;

• Qualité bonne : si la moyenne des notes MOS attribuées est comprise entre 2,8 et 3,9 (MOS º [2,8 ; 3,9]) ;

• Qualité moyenne : si la moyenne des notes MOS attribuées est comprise entre 2,2 et 2,7 (MOS ° [2,2 ; 2,7]) ;

• Qualité mauvaise : si la moyenne des notes MOS attribuées est inférieure à 2,2 (MOS < 2,2) ;

12. Zone : Regroupement des localités et axes routiers tel que défini à l'annexe 2.

Art. 4 : Obligations de réalisation des mesures de qualité de service

Chaque opérateur prend en charge financièrement, chaque année, sur son réseau, la réalisation de mesures de la qualité de service et de la qualité d'expérience, conformément à une méthodologie définie par l'Autorité de régulation. Les opérateurs peuvent être associés à la définition de la méthodologie.

Toutefois, ces mesures peuvent être menées conjointement par l'ensemble des opérateurs et l'Autorité de régulation sur la base du protocole défini par l'Autorité de régulation.

Art. 5 : Contrôle ou audit de qualité de service par l'Autorité de régulation

Dans le cadre de ses missions de contrôle, l'Autorité de régulation réalise ou fait réaliser une fois par an, un audit de la qualité de service sur toute l'étendue du territoire. Le coût de cet audit est à la charge du régulateur.

En outre, l'Autorité de régulation peut réaliser des contrôles continus ou inopinés pendant toute l'année.

En cas de manquements constatés, l'Autorité de régulation, peut réaliser ou faire réaliser aux frais de l'opérateur, des contrôles ou audits supplémentaires.

Art. 6 : Publication des résultats

Les résultats des mesures réalisées par les opérateurs sont transmis à l'Autorité de régulation et publiés selon un format qu'elle définit.

L'Autorité de régulation publie les résultats des mesures qu'elle réalise.

Art. 7 : Modification

Les indicateurs de qualité de service et leurs seuils peuvent être modifiés.

Le Ministère chargé des Communications électroniques peut, le cas échéant, procéder à un appel public à commentaires à titre consultatif. L'arrêté de modification est motivé et publié.

Art. 8 : Les protocoles de mesures

Le Directeur général de l'Autorité de régulation publie par décision, les protocoles de mesures des indicateurs de qualité des services.

Art. 9 : Sanctions

Tout manquement aux obligations de qualité de service mises à la charge des opérateurs expose ces derniers aux sanctions prévues à l'article 31 de la Loi sur les communications électroniques.

L'Autorité de régulation fixera le niveau et le degré de la sanction en fonction de la gravité du manquement constaté.

Art. 10 : Annexes

Les annexes font partie intégrante du présent arrêté.

Art. 11 : Abrogation

Le présent arrêté abroge l'arrêté n0005/MENTD/CAB du 29 avril 2021 portant définition des indicateurs de qualité des services mobiles 2G, 3G et 4G et leurs seuils.

Art. 12 : Entrée en vigueur

Le présent arrêté prend effet à compter de la date de sa signature.

Art. 13 : Exécution

Le directeur général de l'Autorité de régulation des communications électroniques et des postes est chargé de l'exécution du présent arrêté qui sera publié au Journal Officiel de la République Togolaise.

Fait à Lomé, 12 août 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

5. Services de transmission de données (Téléchargements Internet par FTP)

Code	Indicateur	Définition	Seuil	
			3G	4G
TD1	Débit montant (uplink)	Débit de transferts montants (Upload) d'un fichier de 5 Mo vers un serveur donné pour au moins 95% des mesures	≥ 2 Mbps	≥ 12 Mbps
TD2	Débit descendant (downlink)	Débit de transferts descendants (Download) d'un fichier de 10 Mo vers un serveur donné pour au moins 95% des mesures	≥ 3 Mbps	≥ 25 Mbps
TD3	Taux de succès de transfert montant (uplink)	Taux de succès de transferts montants (upload) de fichiers de 5 mégaoctets intégralement effectués.	≥ 96%	≥ 99%
TD4	Taux de succès de transfert descendant (downlink)	Taux de succès de transferts descendants (Download) de fichiers de 10 mégaoctets intégralement effectués.	≥ 96%	≥ 99%
TD5	Taux de coupure ou d'interruption de connexion Data	Taux de coupure des connexions Data, relevé à l'OMC-R	≤ 2%	≤ 1%

6. Infrastructures de réseau

Code	Indicateur	Définition	Seuil (2G, 3G et 4G)
DR1	Nombre d'indisponibilité d'une station de base	Nombre de fois qu'une même station de base est restée indisponible pour une durée d'au moins une heure pendant les 30 derniers jours.	≤ 2
DR2	Délai d'indisponibilité d'une station de base	Délai d'indisponibilité par jour d'une même station de base quel que soit le lieu de son implantation sur le territoire national.	≤ 3H

7. Indicateurs commerciaux

Code	Indicateur	Définition	Seuil
IC1	Taux de rétablissement de cartes SIM en 24 heures	Taux de cartes SIM rétablies au plus tard 24 heures après la signalisation de dysfonctionnement, sur la période considérée. *NB : Le rétablissement d'une carte SIM peut aussi consister en son remplacement*	100%
IC2	Taux de traitement des réclamations en moins de 7 jours	Taux de réclamations traitées en moins de 7 jours après leur enregistrement, sur la période considérée.	≥ 95%

ANNEXES

ANNEXE 1 : INDICATEURS DE QUALITE DES SERVICES DE COMMUNICATIONS ELECTRONIQUES MOBILES 2G, 3G, 4G, LEURS DEFINITIONS ET SEUILS

1. Services Voix mobile

Code	Indicateur	Définition	Seuil (2G, 3G et 4G)
SV1	Délai d'établissement d'appel	Délai au bout duquel une tentative d'appel donne lieu à un retour de sonnerie d'appel	≤ 8 s pour au moins 98% des appels établis
SV2	Taux de succès d'appels	Taux d'appels établis et maintenus pendant 120 secondes	≥ 98%
SV3	Qualité vocale	Note MOS des appels établis et maintenus pendant 120 secondes.	≥ 3,5 pour la moyenne des mesures
SV4	Taux de coupure d'appels (Call Drop Rate)	Taux d'appels établis, puis interrompus indépendamment du fait de l'appelé ou de l'appelant (Call Drop), relevé à l'OMCR.	≤ 1%

2. Services SMS

Code	Indicateur	Définition	Seuil (2G, 3G et 4G)
SMS	Taux de succès de réception de SMS	Taux de SMS envoyés et reçus par le numéro de destination en moins de 10 secondes	≥ 99%

3. Services USSD

Code	Indicateur	Définition	Seuil (2G, 3G et 4G)
USSD	Taux de succès de requêtes USSD	Taux de requêtes USSD ayant généré une réponse sous forme d'affichage en moins de 5 secondes	≥ 99%

4. Services de navigation Web (http et https)

Code	Indicateur	Définition	Seuil	
			3G	4G
NW1	Taux d'échec de téléchargement de pages Web	Taux de tentatives de téléchargement de pages web interrompus après le début de téléchargement.	≤ 1%	≤ 1%
NW2	Délai de téléchargement d'une page web	Délai qui s'écoule entre l'envoi de la requête de téléchargement d'une page web préalablement définie et son chargement intégral.	≤ 5s	≤ 5s

ANNEXE 2 : DEFINITION DES ZONES

ZONE 1 : Capitale et principales villes
Il s'agit de :

- Lomé ;
- Toute l'étendue de la préfecture du Golfe et un rayon de 30 kilomètres autour de l'hôtel de ville de Lomé (tenant compte des contraintes de la zone frontalière avec le Ghana) ;
- Les chefs-lieux de préfecture ;
- La préfecture maritime

ZONE 2 : Zones de développement économique

Les zones concernées sont les suivantes :

· les zones à activités économiques significatives notamment par la présence de ports, d'aéroports, de sources d'énergie, d'usines d'extraction minière, d'unités de transformation agricole, d'agropoles, de parcs industriels ou de marchés à caractère régional ;
· les zones touristiques à forte affluence;
· les zones identifiées par l'Etat pour accueillir des activités économiques et/ou touristiques.

ZONE 3 : Axes routiers prioritaires et principaux

Les axes routiers prioritaires sont les suivants :

· Les routes régionales: routes reliant deux ou plusieurs chefs-lieux de préfectures qu'elles soient dans une même région ou non ;
· Les routes interrégionales : routes reliant deux chefs-lieux de région ;
· Les routes nationales : routes reliant deux frontières internationales.

ZONE 4: Localités rurales à forte densité

Il s'agit de zones rurales qui ne sont pas prises en compte par le service universel et qui ont une importance administrative ou un niveau de population considéré comme important par rapport à la moyenne. Il s'agit notamment de :

· Les chefs-lieux de cantons, hors zones 1 et 2 ;
· Les villages de plus de 2 000 habitants.

ZONE 5 : localités couvertes dans le cadre de la réalisation du service universel

ARRETE N° 006/MENTD DU 12/08/2022
fixant les modalités de modification des cahiers des charges des opérateurs de communications électroniques

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Vu la Constitution du 14 octobre 1992 ;

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2011-178/PR du 07 décembre 2011 fixant les principes généraux d'organisation des départements ministériels ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'État et ministres ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques, modifié par le décret n° 2018-145/PR du 03 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques, modifié par le décret n° 2018-144/PR du 03 octobre 2018 ;

Vu le décret n° 2015-091 du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du gouvernement complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

ARRETE :

CHAPITRE 1er : DISPOSITIONS GENERALES

Article premier : Objet

Le présent arrêté a pour objet de préciser les modalités de modification des cahiers des charges des opérateurs de communications électroniques en application de l'article 13 de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n° 2013-003 du 19 février 2013 et de l'article 19 du décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques

applicables aux activités de communications électroniques, modifié par le décret n° 2018-145/PR du 03 octobre 2018.

À ce titre, il détermine les règles relatives à l'examen de la pertinence des dispositions des cahiers des charges compte tenu de l'évolution du secteur des communications électroniques et des enjeux socio-économiques du pays, ainsi que la procédure pouvant conduire, le cas échéant, à la modification de ces dispositions.

Art. 2 : Champ d'application

Le présent arrêté s'applique à l'ensemble des opérateurs de communications électroniques titulaires d'une licence au Togo.

Art. 3 : Principes gouvernant la modification des cahiers des charges

Les modifications des cahiers des charges doivent notamment être objectivement justifiées et respecter l'équilibre économique des opérateurs, conformément à l'article 13 de la loi n° 2012-018 du 17 décembre 2012 sur les Communications électroniques telle que modifiée par la loi n° 2013-003 du 19 février 2013, à l'article 19 du décret n° 2014-088/PR portant sur les régimes juridiques applicables aux activités de communications électroniques, modifié par le décret n° 2018-145/PR du 03 octobre 2018 et aux dispositions de la licence des opérateurs de communications électroniques.

Lorsque l'Autorité de régulation et/ou le ministère chargé des communications électroniques propose et/ou décide de modifier un ou plusieurs cahiers des charges, ils veillent au traitement équitable, dans des conditions similaires, des opérateurs de communications électroniques qui exercent des activités sur le même marché.

CHAPITRE II : INITIATIVE ET IDENTIFICATION DES MODIFICATIONS A APPORTER AUX CAHIERS DES CHARGES

Art. 4 : Etablissement d'un rapport sur les évolutions du secteur des communications électroniques à l'initiative de l'Autorité de régulation

L'Autorité de régulation peut, de sa propre initiative, en cas de besoin et en raison de l'évolution du secteur des communications électroniques, préparer et communiquer au ministre chargé des communications électroniques, un rapport faisant état des évolutions du secteur des communications électroniques motivant la modification d'un ou de plusieurs cahiers des charges. Le rapport prend notamment en considération les enjeux stratégiques suivants :

- les difficultés techniques rencontrées, endogènes aux réseaux et services de communications électroniques et qui ont porté atteinte au bon fonctionnement et à la qualité des réseaux et services de communications électroniques, l'ordre et la sécurité publics ou aux exigences de la défense nationale ;
- les nouvelles exigences dans les domaines de la sécurité publique ou de la défense nationale ou encore résultant d'un changement à l'échelle internationale ;
- les évolutions technologiques observées ou envisagées par les opérateurs de communications électroniques ou pour le secteur des communications électroniques ;
- le développement des infrastructures et services de communications électroniques au Togo ;
- les exigences environnementales en application des dispositions légales et règlementaires en vigueur et des engagements auxquels a souscrit l'État ;
- les aménagements numériques du territoire en cours ou envisagés et les perspectives de développement économique ;
- la digitalisation des services publics et de l'économie ;
- toute autre considération pertinente, notamment sur le plan socio-économique ou encore démographique.

Dans son rapport visé à l'article 4 du présent arrêté, l'Autorité de régulation pourra :

Art. 5 : Proposition des modifications à apporter aux cahiers des charges

- identifier les dispositions du ou des cahiers des charges dont la modification permettra de répondre aux enjeux stratégiques mentionnés à l'article ~ du présent arrêté ;
- indiquer les modifications qui pourraient être apportées au(x) cahier(s) des charges concerné(s) afin de les adapter à ces enjeux;
- identifier et détailler les motifs qui permettent de justifier objectivement de telles modifications conformément aux dispositions légales et règlementaires applicables ; et
- expliquer en quoi les modifications proposées sont sans effet sur l'équilibre économique de l'opérateur ou des opérateurs concernés.

Art. 6 : Recueil des documents et informations nécessaires à l'établissement du rapport

Pour ta préparation de son rapport visé à l'article 4 du présent arrêté, l'Autorité de régulation peut solliciter auprès des opérateurs de communications électroniques ou auprès de toute administration les documents et informations utiles à ses travaux.

Art. 7 : Envoi du rapport au ministre chargé des communications électroniques

Sur la base du rapport visé à l'article 4 du présent arrêté, le ministre chargé des communications électroniques peut décider de refuser ou d'accepter les modifications proposées au(x) cahier(s) des charges concerné(s). Le cas échéant, le ministre chargé des communications électroniques notifie à l'Autorité de régulation les modifications qu'il envisage d'apporter au(x) cahier(s) des charges concerné(s).

Art. 8 : Demande de modification à l'initiative du ministre chargé des Communications électroniques

Conformément aux dispositions légales et règlementaires applicables, et notamment la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques telle que modifiée par la loi n° 2013-003 du 19 février 2013, le décret n° 2014-088/PR portant sur les régimes juridiques applicables aux activités de communications électroniques, modifié par le décret n° 2018-145/PR du 03 octobre 2018, les dispositions de la licence des opérateurs de communications électroniques, et en fonction des enjeux stratégiques du gouvernement en matière notamment de l'économie numérique, de l'inclusion numérique, des évolutions technologiques et de la digitalisation, le ministre chargé des communications électroniques peut, à tout moment, après consultation de l'Autorité de régulation, prendre l'initiative de proposer la modification du ou des cahier(s) des charges des opérateurs de communications électroniques concernés.

Le cas échéant, le ministre chargé des Communications électroniques notifie à l'Autorité de régulation le projet de modification du ou des cahier(s) des charges concerné(s).

CHAPITRE III : NOTIFICATION AUX OPERATEURS DE COMMUNICATIONS ELECTRONIQUES

Art. 9 : Notification

Dans un délai d'un (1) mois à compter de la notification par le ministère chargé des Communications électroniques de l'Autorité de régulation, celle-ci notifie à l'opérateur ou aux opérateurs de communications électroniques concernés par courrier recommandé avec accusé de réception, les propositions de modifications des cahiers des charges.

L'Autorité de régulation joint les documents suivants à sa lettre de notification :

- le rapport de l'Autorité de régulation visé à l'article 4 du présent arrêté ou tout autre document motivant la modification ou les modifications envisagées ;
- les mesures transitoires proposées par le ministère chargé des communications électroniques et le calendrier y afférent, le cas échéant ;
- le projet de modification du ou des cahier(s) des charges.

Art. 10 : Contenu de la notification

La lettre de notification précise les modalités dans lesquelles l'opérateur ou les opérateurs peuvent présenter leurs observations.

Art. 11 : Délai de réponse

Sauf en cas d'urgence ou en cas de circonstance exceptionnelle, le délai fixé pour permettre aux opérateurs de présenter leurs observations ne peut être inférieur à vingt (20) jours.

CHAPITRE IV -DISCUSSIONS SUR LES PROJETS DE MODIFICATIONS

Art. 12 : Engagement des discussions avec les opérateurs

Après réception des observations de l'opérateur ou des opérateurs de communications électroniques concernés, l'Autorité de régulation engage des discussions avec l'opérateur ou les opérateurs concerné(s) en vue de déterminer les modalités selon lesquelles de telles modifications pourraient être réalisées.

Les discussions entre l'Autorité de régulation et l'opérateur ou les opérateurs concernés doivent respecter le principe du contradictoire et de la transparence. Lorsque l'Autorité de régulation envisage de soulever un argument, elle doit mettre l'opérateur ou les opérateurs concerné(s) en mesure de s'expliquer sur ce point.

Le résultat des discussions est constaté dans un procès-verbal signé par toutes les parties.

Art.13 :Transmission des résultats des discussions au ministre chargé des Communications électroniques

A l'issue des discussions avec l'opérateur ou les opérateurs concerné(s), l'Autorité de régulation adresse au ministre chargé des Communications électroniques un rapport contenant notamment :

- le procès-verbal des discussions ; et
- la mise à jour du projet de cahier(s) des charges modifié(s).

Dans l'hypothèse où l'Autorité de régulation et l'opérateur ou les opérateurs concerné(s) ne parviennent pas à un accord, l'Autorité de régulation explique dans le rapport visé

dans le présent article les raisons du désaccord.

Après réception du rapport, le ministre chargé des Communications électroniques donne des orientations pour finalisation des discussions.

A l'issue des dernières discussions qui font suite à l'orientation donnée par le ministre chargé des communications électroniques, l'Autorité de régulation adresse au ministre chargé des Communications électroniques le rapport visé au premier alinéa revu contenant notamment :

- le procès-verbal des discussions ;
- la mise à jour du projet de cahier(s) des charges modifié(s).

Le ministre chargé des Communications électroniques peut approuver ou refuser les modifications proposées au projet de cahier(s) des charges de l'opérateur ou des opérateurs concerné(s).

Le cas échéant, le ministre chargé des Communications électroniques adresse à l'Autorité de régulation les modifications qui sont apportées au(x) cahier(s) des charges de l'opérateur ou des opérateurs concerné(s).

Art. 14 : Signature des cahiers des charges

L'Autorité de régulation met à jour le projet de cahier(s) des charges et notifie la version définitive à l'opérateur ou aux opérateurs concerné(s) ainsi que les motifs qui justifient objectivement ces modifications.

Le cahier des charges modificatif est signé entre l'Autorité de régulation et l'opérateur concerné.

L'opérateur dispose d'un délai de quinze (15) jours à compter de la notification pour signer le cahier des charges modifié. Si l'opérateur concerné ne signe pas le cahier des charges à l'expiration du délai de quinze (15) jours visé à l'alinéa précédent. le ministre chargé des Communications électroniques rend exécutoire par arrêté le cahier des charges modifié.

CHAPITRE VI- DISPOSITIONS FINALES

Art. 15 : Exécution

Le secrétaire général du ministère de l'Economie Numérique et de la Transformation Digitale et le directeur de l'Autorité de régulation des communications électroniques et des postes sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté qui sera publié au Journal tfficiel de la République Togolaise.

Fait à Lomé, le12 août 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

ARRETE N° 007/MENTD/CAB DU 12/08/2022 portant sur le partage d'infrastructures passives des opérateurs exploitants de réseaux de communications électroniques et des exploitants d'infrastructures alternatives

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'Etat et ministres ;

Vu le décret n° 2012-006/PR du 7 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par le décret n° 2018-145/PR du 3 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du gouvernement complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu le décret n° 2020-116/PR du 23 décembre 2020 portant sur le déploiement national de réseaux de communications électroniques en fibre optique ;

ARRETE :

CHAPITRE 1 : DES DISPOSITIONS GENERALES

Article premier : Objet

Le présent arrêté détermine les règles applicables :

- au partage des infrastructures passives des opérateurs exploitants de réseaux de communications électroniques et des exploitants d'infrastructures alternatives ;
- à la sécurisation et à la redondance des câbles sous-marins de fibre optique et des réseaux nationaux de fibre optique terrestre (backbones) ;
- à la fourniture d'information et l'établissement d'une cartographie relative aux infrastructures passives des opérateurs exploitants de réseaux de communications électroniques et des exploitants d'infrastructures alternatives ;
- à l'installation ou au renforcement des infrastructures passives des opérateurs exploitants de réseaux de communications électroniques et des exploitants d'infrastructures alternatives.

Les dispositions qui suivent, complètent celles de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013, du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 et du décret n° 2020-116/PR du 23 décembre 2020 portant sur le déploiement national de réseaux de communications électroniques en fibre optique.

Art. 2 : Champ d'application

Le présent arrêté s'applique aux opérateurs exploitant un réseau de communications électroniques ouvert au public ainsi qu'aux exploitants d'infrastructures alternatives.

Art. 3 : Définitions

Les termes employés dans le présent arrêté ont la signification que leur confèrent l'article 4 de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013 ; l'article 4.2 du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 ainsi que l'article 2 du décret n° 2020-116/PR du 23 décembre 2020 portant sur le déploiement national de réseaux de communications électroniques en fibre optique.

CHAPITRE II : REGLES DE PARTAGE DES INFRASTRUCTURES PASSIVES DES OPERATEURS EXPLOITANTS DE RESEAUX DE COMMUNICATIONS ELECTRONIQUES ET DES EXPLOITANTS D'INFRASTRUCTURES AL TERNATIVES

Art. 4 : Principes généraux

Les opérateurs exploitant un réseau de communications électroniques ouvert au public et les exploitants d'infrastructures alternatives sont tenus de faire droit aux demandes raisonnables de partage de leurs infrastructures passives de tout opérateur.

Tout refus de faire droit à une demande de partage des infrastructures passives est motivé.

La demande de partage des infrastructures passives d'un opérateur exploitant un réseau de communications électroniques ouvert au public ne peut être refusée que si l'opérateur n'as pas la capacité technique de la satisfaire.

La demande de partage des infrastructures passives d'un exploitant d'une infrastructure alternative ne peut être refusée que si le refus est fondé sur des critères objectifs, transparents et proportionnés, tels que :

· la capacité technique des infrastructures passives à accueillir des éléments du réseau de communications électroniques, en raison notamment du manque d'espace disponible, y compris pour des besoins futurs d'espace qui ont été démontrés de manière suffisante ;

· la sécurité nationale, la sécurité publique, la santé publique ou la sécurité des personnes ;

· l'intégrité et la sécurité du réseau de l'opérateur ;

· les risques de perturbation grave de l'infrastructure passive ;

· la disponibilité d'autres offres de gros d'accès à des infrastructures passives de l'exploitant d'infrastructures alternatives, adaptées au déploiement de réseaux de communications électroniques, auxquelles l'accès est offert selon des modalités et conditions équitables et raisonnables ;

· les obligations issues de réglementation particulières applicables à l'exploitant d'infrastructures alternatives.

Art. 5 : Partage des infrastructures passives des opérateurs exploitant un réseau de communications électroniques ouvert au public

Les opérateurs exploitant un réseau de communications électroniques ouvert au public sont tenus de privilégier toute solution de partage des infrastructures passives techniquement faisable et économiquement rentable dans le cadre du déploiement de leurs réseaux.

Avant de construire une nouvelle infrastructure passive, l'opérateur exploitant un réseau de communications électroniques ouvert au public s'assure de l'absence d'une infrastructure passive dans des conditions permettant le partage dans un périmètre précisé par décision de l'Autorité de régulation.

Les opérateurs exploitant un réseau de communications électroniques ouvert au public doivent veiller à ce que les conditions d'établissement de chacune des infrastructures passives rendent possible l'accueil ultérieur d'installations d'autres opérateurs notamment à travers des prestations de location de liaisons en fibre optique, de colocalisation (pylônes, terrasses ou sites), d'appui sur poteaux, d'accès au génie civil (conduites, alvéoles, chambre).

Les infrastructures passives et actives financées par le fonds du service universel doivent être conçues et construites de façon à pouvoir être partagées avec les autres opérateurs.

Art. 6 : Partage des infrastructures passives des exploitants d'infrastructures alternatives

Lorsqu'un exploitant d'infrastructures alternatives reçoit une demande de partage de ses infrastructures, il est tenu d'examiner la demande dans des conditions objectives, transparentes et non-discriminatoires.

Il communique sa réponse à l'opérateur dans un délai maximal d'un (01) mois à compter de la réception d'une demande complète.

Les conditions de cet accès font l'objet d'une convention entre l'opérateur et l'exploitant d'infrastructures alternatives précisant son étendue et les obligations mutuelles.

La convention de partage des infrastructures alternatives est notifiée à l'Autorité de régulation au plus tard dans les huit (8) jours calendaires suivant sa conclusion.

L'Autorité de régulation dispose d'un délai de trois (3) mois, à compter de la réception de la convention, pour demander sa modification. La convention modifiée est notifiée à l'Autorité de régulation selon les mêmes modalités.

Art. 7 : Principes applicables aux offres de référence de partage des infrastructures passives des opérateurs exploitants un réseau de communications électroniques ouvert au public

Les opérateurs exploitant un réseau de communications électroniques sont tenus de publier et de mettre annuellement à jour une offre de référence de partage des infrastructures passives qui sera incluse dans leur catalogue d'interconnexion et d'accès.

Le contenu minimum de l'offre de référence de partage des infrastructures passives est précisé par arrêté du ministre en charge des communications électroniques.

L'offre de référence de partage des infrastructures passives est soumise à l'Autorité de régulation pour approbation.

L'offre de référence de partage des infrastructures passives doit être proposée dans des conditions économiques, techniques et d'accessibilité raisonnables. Elle respecte le principe d'orientation des prix vers les coûts.

Art. 8 : Conventions de partage des infrastructures passives Les conventions de partage d'infrastructures passives sont de droit privé.

Sans préjudice des dispositions des articles 6 et 11 du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018, les conventions de partage des infrastructures passives doivent comporter au minimum :

· la description complète de «infrastructure, ses caractéristiques techniques et son dimensionnement ;

· les conditions d'accès à l'infrastructure ;

· les conditions de partage de l'infrastructure en termes d'espace, de gestion et de maintenance, notamment la description technique complète des équipements ;

· les conditions commerciales et financières applicables à la convention ;

· les informations que les parties doivent se communiquer de façon régulière pour assurer une bonne gestion de l'infrastructure ;

· les règles de confidentialité à respecter par les parties ;

· la date d'entrée en vigueur, les conditions de renouvellement et la durée de la mise à disposition de l'infrastructure ;

· les conditions de résiliation de la convention de partage des infrastructures passives ;

· les dispositions concernant les procédures de facturation et de recouvrement ainsi que les modalités de paiement ;

· les règles de responsabilité et d'indemnisation en cas de défaillance d'une des parties ;

· les éventuels droits de propriété intellectuelle ;
· les conditions liées au respect des servitudes radioélectriques ;

· les procédures de notification et les coordonnées des représentants habilités de chacune des parties ;

· en tant que de besoin, les conditions de répartition des investissements entre les parties dans le cas où les obligations de partage entraîneraient des investissements supplémentaires de la part de la partie propriétaire ou gestionnaire ;

· les procédures de règlement des litiges avec mention de recours obligatoire à l'Autorité de régulation.

Les dispositions de l'article 10 du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 s'appliquent en cas de refus, d'échec des négociations commerciales ou de désaccord sur la conclusion ou l'exécution d'un accord de partage des infrastructures passives.

Les conventions de partage des infrastructures passives respectent les textes législatifs et réglementaires applicables relatifs à l'interconnexion et l'accès.

CHAPITRE III : SECURISATION ET REDONDANCE DES STATIONS D'ATTERRISSEMENT ET DES RESEAUX NATIONAUX DE FIBRE OPTIQUE TERRESTRE

Art. 9 : Points d'accès et d'interconnexion

Les opérateurs exploitant un réseau de communications électroniques ouvert au public dans Lomé et dans tous les chefs-lieux de préfecture ainsi que dans les localités de la zone 2 *« zone économique spéciale ou ayant un potentiel économique »* qui seront précisées par décision de l'Autorité de régulation, sont tenus d'établir et d'exploiter des points d'accès et d'interconnexion y compris de colocalisation.

L'offre technique et tarifaire relative aux points d'accès et d'interconnexion dans Lomé et dans tous les chefs-lieux de préfecture ainsi que dans les localités de la zone 2 doivent figurer dans le catalogue d'interconnexion et d'accès de ces opérateurs.

Art. 10 : Sécurisation et redondance des câbles sous-marins de fibre optique et des réseaux nationaux de fibre optique terrestre

Tous les exploitants de stations d'atterrissement de câbles sous-marins sont tenus de conclure mutuellement des accords de partage des infrastructures passives leur permettant de re-router leur trafic en cas de coupure de leurs réseaux afin d'assurer le respect de leurs obligations de qualité de service.
Tous les exploitants de réseaux nationaux de fibre optique terrestre sont tenus de conclure mutuellement des accords de partage des infrastructures passives leur permettant de re- router leur trafic en cas de coupure de leurs réseaux afin d'assurer le respect de leurs obligations de disponibilité et de qualité de services.

Le chiffre d'affaires généré par les activités facturés prévues au présent article est exclu de l'assiette permettant le calcul des redevances de régulation prévues dans les cahiers des charges des opérateurs.

Ces accords sont transmis à l'Autorité de régulation pour approbation.

Les dispositions de l'article 10 du décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 s'appliquent en cas de refus, d'échec des négociations commerciales ou de désaccord sur la conclusion ou l'exécution de ces accords.

CHAPITRE IV : FOURNITURE D'INFORMATIONS ET DE CARTOGRAPHIE RELATIVES AUX RESEAUX ET AUX INFRASTRUCTURES DE COMMUNICATIONS ELECTRONIQUES ET SYSTEME D'INFORMATION GEOGRAPHIQUE

Art. 11 : Fourniture d'informations et de cartographie à l'Autorité de régulation sur les réseaux et les infrastructures existants

Les opérateurs et les exploitants d'infrastructures alternatives communiquent à l'Autorité de régulation, dans les conditions, la périodicité et les formats demandés par celle-ci, l'ensemble des informations pertinentes relatives à leurs réseaux de communications électroniques, leurs infrastructures passives et actives et leurs infrastructures alternatives existants au jour de l'entrée en vigueur du présent arrêté.

Art. 12 : Schéma de déploiement prévisionnel des infrastructures passives

Les opérateurs et les exploitants d'infrastructures alternatives élaborent chaque année, un schéma de déploiement prévisionnel de leurs infrastructures passives et alternatives pour l'année civile suivante. Ce schéma est communiqué à l'Autorité de régulation au plus tard le 30 octobre de chaque année.

Art. 13 : Système d'information géographique

Sur la base des informations et des schémas de déploiement prévisionnel visés aux articles 11 et 12, l'Autorité de régulation élabore et tient à jour une base de données et une cartographie prenant la forme d'une base de données :

· des réseaux de communications électroniques ouverts au public ainsi que des infrastructures passives et actives des opérateurs offrant aux autres opérateurs la possibilité de s'y colocaliser ;

· des infrastructures alternatives détenues par les exploitants d'infrastructures alternatives.

Cette base de données doit être interconnectée à la base de données de l'Agence Togo Digital (ATD) et accessible afin de permettre aux différentes parties prenantes de vérifier la disponibilité des infrastructures.

Les conditions d'accès sont définies par l'Autorité de régulation.

CHAPITRE V : OPERATIONS DE TRAVAUX D'INSTALLATION OU DE RENFORCEMENT D'INFRASTRUCTURES PASSIVES

Art.14 : Modalités d'installation des infrastructures

Lors du déploiement des infrastructures en fibre optique, les opérateurs exploitant un réseau de communications électroniques ouvert au public sont tenus de se conformer aux exigences et spécifications techniques définies par le guide de pose d'infrastructures en fibre optique adopté par décision de l'Autorité de régulation.

Art.15 : Information de l'Autorité de régulation des opérations de travaux d'installation ou de renforcement d'infrastructures passives et alternatives

Les opérateurs exploitant un réseau de communications électroniques ouvert au public et les exploitants d'infrastructures alternatives informent par écrit l'Autorité de régulation, au moins quatorze (14) jours ouvrés à l'avance, des opérations de travaux d'installation ou de renforcement des infrastructures passives et alternatives, dès la planification de ces travaux.

A cette fin, ils fournissent les informations suivantes :

· l'emplacement et le type des travaux ;

· les éléments de réseaux concernés ;

· la date estimée de début des travaux et la durée de ces derniers ; et

· un point de contact.

Ces informations sont transmises à l'Autorité de régulation dans un format ouvert, aisément réutilisable et exploitable par un système de traitement automatisé largement répandu, permettant de visualiser, sur un outil cartographique, la zone d'emprise des travaux. Les informations relatives à l'emplacement des travaux et aux éléments de réseaux concernés peuvent être transmises sous forme de données numériques vectorielles géolocalisées pouvant être reprises dans le système d'information géographique visé à l'article 13, suivant un format largement répandu.

Dès la réception des informations visées à l'alinéa premier de l'article 14, l'Autorité de régulation les communique aux exploitants de réseaux ouverts au public ainsi qu'aux exploitants d'infrastructures alternatives dans des conditions objectives, transparentes et non-discriminatoires.

La communication de ces informations à l'Autorité de régulation ne peut être limitée ou refusée que pour les motifs suivants, dûment justifiés :

· la sécurité et l'intégrité des réseaux ;

· la sécurité nationale, la sécurité publique, la santé publique ou la sécurité des personnes ;

· la confidentialité de ces informations ou la protection du secret des affaires.

Les opérateurs exploitant un réseau de communications électroniques ouvert au public et les exploitants d'infrastructures alternatives confirment les informations communiquées à l'Autorité de régulation à l'alinéa 1er de l'article 14, dès l'obtention des droits de passage sur le domaine public et des servitudes sur les propriétés privées. Lorsqu'il est constaté que le droit de passage de l'opérateur peut être assuré par l'utilisation des installations existantes d'un autre occupant du domaine publie, dans des conditions équivalentes à celles qui résulteraient d'une occupation autorisée, l'Autorité de régulation peut inviter les deux parties à se rapprocher pour convenir des conditions techniques et financières d'une utilisation partagée des installations en question et à solliciter les autorisations requises à l'autorité ayant attribué le droit de passage.

CHAPITRE VI : DISPOSITIONS DIVERSES ET FINALES

Art. 16 : Autres mesures

Pour toutes les infrastructures en fibre optique existantes, les opérateurs disposent d'un délai de trois (3) ans à compter de l'entrée en vigueur du présent arrêté, pour se conformer aux dispositions de l'article 14 du présent arrêté.

Art. 17: Entrée en vigueur et publication

Le présent arrêté entre en vigueur à compter de la date de sa signature et sera publié au Journal Officiel de la République Togolaise.

Art. 18 : Exécution

Le directeur général de l'Autorité de régulation des communications électroniques et des postes est chargé de l'exécution du présent arrêté.

Fait à Lomé, le 12 août 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

ARRETE N° 008/MENTD/CAB DU 12/08/2022 portant homologation de la décision de l'ARCEP portant modalités et conditions de mise en œuvre de la portabilité des numéros mobiles

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Vu la loi n° 2012 - 018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013 - 003 du 19 février 2013 ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par le décret n° 2018-145/PR du 3 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n02018-144/PR du 3 octobre 2018 ;

Vu le décret n° 2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de régulation des communications électroniques et des postes ;

Vu le décret n° 2018-174/PR du 10 décembre 2018 fixant les taux, les modalités de recouvrement et d'affectation des redevances dues par les opérateurs et exploitants de réseaux et services de communications électroniques, les fournisseurs d'équipements et terminaux et les installateurs d'équipements radioélectriques ;

Vu le décret n° 2018-070/PR du 18 avril 2018 relatif au service universel des communications électroniques ;

Vu le décret n° 2020-023-PR du 07 avril 2020 portant nomination des membres du comité de direction de l'ARCEP et de son président ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ; Vu le décret n° 2020-080/PR du 1er octobre 2020 portant composition du gouvernement complété par le décret n° 2020-090/PR du 2 novembre 2020 ;

Vu le décret n° 2020-085/PR du 15 octobre 2020 portant nomination du directeur général de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu l'arrêté n° 005/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l'opérateur Togo Cellulaire pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles ;

Vu l'arrêté n° 006/MPEN/CAB du 12 juin 2018 portant extension à la 4G et renouvellement de la licence de l'opérateur Atlantique Telecom Togo pour l'établissement et l'exploitation de réseaux de réseaux de communications électroniques mobiles ;

Vu le cahier des charges de l'opérateur Togo Cellulaire du 22 novembre 2019 pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles 2G, 3G et 4G ;

Vu la décision n° 2011-002/ART&P/CO du 26 avril 2011 portant adoption du plan national de numérotation ;

Vu la décision n° 137/ARCEP/DG/22 du 18 juillet 2022 portant modalités et conditions de mise en œuvre de la portabilité des numéros mobiles.

ARRETE :

Article premier : Objet

Le présent arrêté porte homologation de la décision n° 137/ ARCEP/OG/22 du 18 juillet 2022 de l'Autorité de régulation des communications électroniques et des postes (ARCEP), portant modalités et conditions de mise en œuvre de la portabilité des numéros mobiles.

Ladite décision est jointe en annexe du présent d'arrêté et en fait partie intégrante.

Art. 2 : Entrée en vigueur

Le présent arrêté prend effet à compter de la date de sa signature.

Art. 3 : Exécution

Le directeur général de l'Autorité de régulation des communications électroniques et des postes est autorisé à publier la décision en Annexe du présent arrêté.

Le présent arrêté sera publié au Journal Officiel de la République Togolaise.

Fait à Lomé, le 12 août 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

ARRETE N° 009 /MENTD/CAB DU 12/08/2022 portant régime de l'autorisation spéciale pour la fourniture des services d'interconnexion intranet boucle locale radio

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE

Sur rapport du directeur général de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'Etat et ministres ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par le décret n° 2018-145/PR du 3 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 03 octobre 2018 ;

Vu le décret n° 2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de Régulation des communications électroniques et des postes (ARCEP) ;

Vu le décret n° 2018-174/PR du 10 décembre 2018 fixant les taux, les modalités de recouvrement et d'affectation des frais et redevances dus par les opérateurs et exploitants de réseaux et services de communications électroniques, les fournisseurs d'équipements et terminaux et les installateurs d'équipements radioélectriques ;

Vu le décret n° 2020-023/PR du 07 avril 2020 portant nomination des membres du comité de direction de l'Autorité de Régulation des Communications Electroniques et de Postes (ARCEP) et de son président ;

Vu le décret n° 2020-076/PR du 28 septembre 2020 portant nomination du Premier ministre ;

Vu le décret n° 2020-080/PR du 1 er octobre 2020 portant composition du gouvernement ;

Vu le décret n° 2020-085/PR du 15 octobre 2020 portant nomination du directeur général de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;

ARRETE :

Article premier : Objet

Conformément à l'article 21 du décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par décret n° 2018-145/PR du 3 octobre 2018, le présent arrêté, a pour objet d'ériger un régime d'autorisation spéciale applicable aux fournisseurs des services d'interconnexion intranet Boucle Locale Radio (BLR).

Art. 2 : Champ d'application

Le présent arrêté s'applique à l'établissement et à l'exploitation de réseau point à point et point à multi points, pour la fourniture des services d'interconnexion intranet BLR, aux établissements, agences, filiales, succursales, départements et services ou d'autres institutions partenaires tous installés sur le territoire national.

Art. 3 : Bandes de fréquences

Les fréquences mises en œuvre pour la fourniture des services visés par le présent arrêté sont des fréquences libres. Les bandes sont précisées par décision de l'Autorité de régulation.

Art. 4 : Demande d'autorisation spéciale

La demande d'autorisation spéciale adressée au ministre chargé des communications électroniques est déposée à l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) qui en assure l'instruction.

Les pièces constitutives de la demande sont précisées par décision de l'Autorité de régulation.

Art. 5 : Durée de l'autorisation

L'autorisation est accordée par arrêté du ministre chargé des communications électroniques pour une durée de cinq (5) ans, renouvelable.

Art. 6 : Eléments constitutifs de l'autorisation

L'autorisation pour la fourniture de services d'interconnexion

intranet BLR est constituée des éléments suivants :

· un arrêté du ministre portant autorisation spéciale de fourniture de services d'interconnexion intranet ;
· un cahier des charges signé entre le titulaire et l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;
· une décision d'assignation de fréquences, si le demandeur a besoin, pour la fourniture de ses services, des fréquences soumises à autorisation.

Art. 7 : Frais et redevances liées à l'autorisation

Le titulaire est tenu, conformément à la réglementation en vigueur, au paiement des frais et redevances ci-après :

· Redevance annuelle d'exploitation fixée à 3% du chiffre d'affaires ;
· Redevance d'autorisation spéciale ou de renouvellement fixée à dix millions (10 000 000) F CFA ;
· Redevance annuelle forfaitaire de gestion et de contrôle de fréquences le cas échéant ;
· Redevances annuelles d'utilisation des fréquences le cas échéant ;
· Frais d'études de dossier fixés à cinq cent mille (500 000) F CFA.

Art. 8 : Obligations du titulaire

Tout titulaire d'autorisation spéciale pour la fourniture d'interconnexion intranet BLR est tenu au respect des règles et obligations prévues par le cadre légal et réglementaire, ainsi qu'à son cahier des charges.

Tout manquement expose le titulaire aux sanctions prévues par la réglementation en vigueur.

Art. 9 : Entrée en vigueur

Le présent arrêté prend effet à compter de la date de sa signature.

Art. 10 : Exécution

Le directeur général de l'Autorité de régulation des communications électroniques et des postes est chargé de l'exécution du présent arrêté qui sera publié au Journal Officiel de la République Togolaise.

Fait à Lomé, le 12 août 2022

Le ministre de l'Economie Numérique et de la Transformation Digitale

Cina LAWSON

DECISION N° 137/ARCEP/DG/22 DU 18/07/2022 portant modalités et conditions de mise en œuvre de la portabilité des numéros mobiles

LE DIRECTEUR GENERAL DE L'AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES

Vu la loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, telle que modifiée par la loi n° 2013-003 du 19 février 2013 ;

Vu le décret n° 2020-085/PR du 15 octobre 2020 portant nomination du Directeur Général de l'Autorité de régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu le décret n° 2020-023/PR du 07 avril 2020 portant nomination des membres du Comité de Direction de l'ARCEP et de son Président ;

Vu le décret n° 2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur J'interconnexion et l'accès aux réseaux des communications électroniques modifié par le décret n° 2018-144/PR du 3 octobre 2018 ;

Vu la décision n° 173/ART&P/DG/19 du 25 octobre 2019, déterminant les règles de gestion du plan national de numérotation ;

Vu la décision n° 2011-002/ART&P/CD du 26 avril 2011 portant adoption du plan national de numérotation ;

Considérant les conclusions de l'étude de marché, effectuée par l'ARCEP en concertation avec les opérateurs mobiles, pour l'évaluation des besoins des Abonnés de services mobiles de communications électroniques en matière de Portabilité afin d'identifier les catégories de consommateurs susceptibles de demander ce service ;

Vu la concertation menée avec les opérateurs mobiles relative au projet de Portabilité des numéros au Togo, du mois de décembre 2021 ;

Vu les résultats de la concertation susvisée ;

Considérant que :

• La portabilité des numéros est définie par l'article 4 de la loi n° 2012-018 sur les communications électroniques du 17 décembre 2012 modifiée comme « la possibilité pour un usager, abonné à un fournisseur de services de communications électroniques, lorsqu'il change de fournisseur de conserver le même numéro géographique sans changer d'implantation géographique et, de conserver son numéro non géographique, fixe ou mobile lorsqu'il change de fournisseur tout en restant au Togo ».

• L'article 36 nouveau de la loi n° 2012-018 susmentionnée fixe les principales étapes de la mise en œuvre de la portabilité des numéros :

a) L'ARCEP doit procéder à une étude de marché qui doit avoir pour objet d'évaluer les besoins des abonnés mobiles en matière de portabilité afin d'identifier les catégories d'abonnés mobile susceptibles de demander ce service ;

b) Lorsque l'étude de marché conclut à un besoin clairement identifié, il revient à l'ARCEP de mettre en place un dispositif adapté pour permettre au consommateur de conserver son numéro ;

c) Les modalités de mise en œuvre de la portabilité des numéros sont alors adoptées par décision de l'Autorité de régulation, homologuée préalablement par le Ministre chargé des Communications électroniques après concertation avec les opérateurs.

• L'étude de marché réalisée par l'ARCEP en octobre 2021 démontre que 95% des répondants souhaitent conserver leur numéro s'ils venaient à changer de fournisseur de service mobile avec une forte préférence pour des délais de Portage de moins d'une journée et un service gratuit.

De même, 70% des interrogés se disent ennuyés s'ils devaient changer leur Numéro .de Mobile.

Cette étude montre que les effets positifs de la Portabilité des numéros sur le marché sont nombreux, à savoir :

- impact direct sur la baisse des prix des communications, développement des. remises sur les communications en contrepartie du développement des engagements avec un opérateur, et du développement des offres promotionnelles ;
- impact direct sur le développement d'une concurrence accrue sur le marché ;
- impact direct sur l'amélioration de la qualité des services ;
- impact direct sur le développement des services innovants.

Il résulte également de cette étude que la forte tendance des abonnés mobile à détenir chacun au moins une carte SIM et un numéro de mobile auprès de chaque opérateur ne constitue pas un facteur disqualifiant pour un projet de portabilité.

En effet, cette pratique dite «multi-SIM» est une réponse de l'Abonné .à des facteurs défavorables tels qu'une qualité de couverture inégale entre les deux opérateurs sur une même zone géographique. Elle pénalise l'abonné qui doit supporter indéfiniment la multiplication des coûts, ainsi que les pertes et difficultés de gestion découlant de cette pratique.

Au contraire, la mise en œuvre de ladite portabilité est de nature à permettre, à terme, de résorber cette tendance défavorable au consommateur tout en favorisant une amélioration de la qualité de service.

En outre, l'essor de certains services à forte valeur ajoutée tels que le paiement mobile et l'utilisation du mobile comme facteur d'authentification dans le cadre de l'e-commerce et de l'e-administration renforce le lien entre l'abonné et son numéro mobile. Le développement d'une identité directement vérifiable et utilisable dans le cadre des services Internet constitue l'un des facteurs de succès de l'économie numérique. Faire du numéro mobile un identifiant unique représente donc un enjeu de taille au niveau national.

Au total, il résulte de l'étude menée par l'ARCEP, un réel et fort intérêt, voire une nécessité pour l'abonné mobile de conserver son numéro en cas de changement d'opérateur. Sur la base de cette étude, l'ARCEP conclut donc à l'existence d'un besoin clairement identifié en matière de portabilité des numéros mobiles et ce, pour toutes les catégories de consommateurs susceptibles de demander ce service.

L'ARCEP estime que le marché de la téléphonie fixe n'appelle pas à la date des présentes, l'examen de l'opportunité d'un dispositif de Portabilité autre que la portabilité .géographique déjà mise en œuvre. L'ARCEP se réserve toutefois la possibilité de procéder à un tel examen au regard notamment de l'évolution du marché, du comportement des consommateurs ou des solutions technologiques.

DECIDE :

CHAPITRE 1er - DISPOSITIONS GENERALES

Article premier : Objet

La présente décision définit les modalités et conditions de mise en œuvre de la portabilité des numéros mobiles au Togo.

Art. 2 : Champ d'application

La présente décision s'applique aux opérateurs, titulaires de licence pour l'établissement et l'exploitation de réseaux de communications électroniques mobiles au Togo.

Art. 3 : Définitions

Les termes dont la première lettre figure en majuscule dans la présente décision ont la signification que leur confère la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques. Les termes qui n'y sont pas définis auront la signification ci-après.

- Abonné ou Abonné Mobile : personne physique ou morale ayant souscrit à un service fourni par un Opérateur Mobile et à laquelle a (ont) été affecté(s) un ou plusieurs Numéros Mobiles.

- Demande de Portage : demande formulée par l'Abonné auprès de l'Opérateur Receveur afin de mettre en œuvre le Portage de son Numéro Mobile.

- Numéro Mobile : numéro non géographique employé pour la fourniture d'un service de communication interpersonnelles mobiles.

- Opérateur Attributaire : Opérateur Mobile auquel a été attribué le Numéro Mobile objet de la demande de Portage.

- Opérateur Donneur : Opérateur Mobile à partir duquel le Numéro Mobile est porté et qui peut être ou non l'Opérateur Attributaire.

- Opérateur Mobile : Opérateur Attributaire ou bénéficiant d'une mise à disposition de tels numéros.

- Opérateur Receveur : Opérateur Mobile vers lequel le numéro de mobile est porté.

- Portabilité : la possibilité pour un usager, abonné à un fournisseur de services de communication électroniques, lorsqu'il change de fournisseur de conserver-son Numéro Mobile lorsqu'il change de fournisseur tout en restant sur le territoire national.

- Portabilité de Numéros Mobiles (PNM) : service qui permet à un abonné de conserver son numéro mobile en cas de changement d'opérateur de téléphonie mobile.

- Portage : les opérations liées à la mise en œuvre de la Portabilité.

- RIO : Relevé d'Identité Opérateur.

- Serveur d'Information : le serveur d'information mis en place par chaque Opérateur afin de permettre à chaque Abonné de connaitre les informations nécessaires à la réalisation de la Portabilité sur la ligne dont il est titulaire, notamment le RIO et, le cas échéant, de suivre la réalisation de l'opération de Portabilité qu'il a demandé.

CHAPITRE II : PRINCIPES G.ENERAUX DE LA PORTABILITE

Art. 4 : Mise en place de la base de données centralisée
Les données relatives à la Portabilité des Numéros Mobiles de tous les Opérateurs seront contenues dans une base de données centrale et accessible à tous les Opérateurs en temps réel. Celle-ci pourra être dupliquée par chaque Opérateur sur son réseau de manière à accélérer et fiabiliser son interrogation.

Art. 5 : Modalités de gestion de la base de données

Les modalités de gestion de la base de données centralisée seront établies par l'ARCEP qui pourra en confier l'exploitation à un tiers.

Art. 6 : Relevé d'identité opérateur mobile - RIO mobile

Chaque Opérateur Mobile attribue sans délai à chaque Numéro Mobile actif un RIO mobile. Toute modification ultérieure du RIO mobile par l'Opérateur doit être mise à disposition de l'Abonné Mobile dans les 24 heures.

Art. 7 : Routage des appels

Le réseau de l'Opérateur d'origine devra détecter que le Numéro appelé est Porté sur un réseau donné. L'opérateur d'origine devra alors interroger la base de données centralisée afin d'obtenir un numéro de routage. Il acheminera ensuite la communication en direction du réseau receveur avec notamment l'utilisation de la méthode d'acheminement selon les principes d'interrogation systématique (Ali Cali Query-ACQ). Ce dernier se chargera d'achever l'établissement de l'appel.

Pour les communications internationales entrantes à destination des numéros portés, l'opérateur attributaire est tenu d'appliquer le routage indirect pour router ces communications vers l'opérateur receveur.

Art. 8 : Gratuité des services de Portabilité pour les abonnés mobile

La gratuité du service de Portabilité est due aux Abonnés Mobile. Le Portage du Numéro de mobile ne doit représenter aucun coût supplémentaire pour l'Abonné. Aucun frais,

charge ni pénalité ne peut être appliqué au consommateur en conséquence d'une demande dé Portage.

Art. 9 : Guichet unique virtuel pour les abonnés mobile
Chaque Opérateur met en place un « guichet unique » virtuel comme seul point de contact pour les Abonnés Mobile souhaitant conserver leur Numéro. Ce point de contact unique est l'Opérateur Receveur, qui sera chargé de faire le lien avec le ou les autres Opérateurs concernés.

Art. 10 : Délais de Portage

Le délai de Portage est fixé à 2 jours ouvrés à compter de la demande de conservation du Numéro de Mobile formulée par l'Abonné.

La rétractation de la demande de Portage des Numéros est possible à toute moment, jusqu'à un jour ouvrable avant la date prévue du Portage.

Art. 11 : Refus de Portage

Il est reconnu aux opérateurs la possibilité d'opposer un refus à une demande de Portage dans le cas de lignes inactives depuis 90 jours, bloquées, non-identifiées créées, activées ou portées depuis moins de 90 jours.

Art. 12 : Information des Abonnés Mobiles

Chaque Opérateur Mobile met en place le dispositif nécessaire (brochures, conditions générales de vente, site internet, espace client internet, etc.) permettant à tout Abonné de connaître les modalités lui permettant d'exercer son droit à la Portabilité, notamment le délai global de mise en œuvre de la demande de Portage du Numéro Mobile.

Chaque Opérateur met en place un serveur vocal et / ou USSD selon les indications qui seront définies par l'ARCEP permettant gratuitement à chaque consommateur de connaître les informations nécessaires à la réalisation de la Portabilité sur la ligne dont il est titulaire, notamment le RIO et, le cas échéant, de suivre la réalisation de l'opération de Portage qu'il a demandée.

CHAPITRE III : PROCESSUS ET PROTOCOLE DU PORTAGE

Art.13 : Processus opérationnel de Portage

Les Opérateurs prennent les mesures nécessaires pour que le processus qui permet à l'Abonné de conserver son Numéro Mobile en changeant d'Opérateur se déroule selon les étapes décrites ci-après.

13.1. Dans le cadre de la souscription à une offre auprès de l'Opérateur Receveur, l'Abonné présente une demande de conservation du numéro mobile. L'Abonné doit fournir à l'Opérateur Receveur les éléments et informations suivantes :

- Le numéro de téléphone mobile objet de la demande et ;

- Le RIO Mobile.

13.2. L'Opérateur Receveur ne peut refuser la demande de Portage que dans les cas suivants :

- Incapacité du demandeur : la demande de Portage du Numéro Mobile doit être présentée par le titulaire du contrat ou par une personne dûment mandatée par celui-ci ;

- Demande incomplète ou contenant des informations erronées : la demande de Portage doit comporter l'ensemble des informations nécessaires, notamment le Numéro Mobile objet de la demande et le relevé d'identité opérateur mobile (RIO mobile) correspondant ;

- Non-respect des règles de gestion du plan national de numérotation.

L'Opérateur Receveur vérifie l'exactitude de la demande formulée par le titulaire du contrat ou par son mandataire. Il s'assure du bon format et de la cohérence de la clé du RIO Mobile transmis par l'Abonné au moment de la demande de Portage, que celle-ci ait lieu dans un point de vente physique ou par vente à distance.

13.3. L'Opérateur Receveur informe l'Abonné Mobile des conséquences de sa demande de Portage. Il rappelle notamment à l'Abonné Mobile :

- Qu'il lui revient, s'il le souhaite, de fixer une date d'effet de la Portabilité, correspondant à la date d'expiration du crédit disponible auprès de l'Opérateur Donneur, en cas d'offre prépayée, afin d'éviter de perdre ledit crédit ;

- Qu'il lui revient d'utiliser la totalité des sommes disponibles sur le compte de paiement mobile attaché au Numéro objet de la portabilité ou de réaliser en temps utile les démarches nécessaires au transfert desdites sommes vers l'Opérateur Receveur afin que l'Abonné Mobile puisse en disposer lorsque cette possibilité lui reconnue par les textes applicables ;

L'Opérateur Receveur est le seul interlocuteur de l'Abonné Mobile concernant sa demande de Portage. Les informations délivrées à l'Abonné Mobile concernent au minimum les éléments suivants :

- le droit à la Portabilité est soumis à des critères d'éligibilité notamment que le numéro porté soit toujours actif le jour du Portage ;

- la demande de Portage du numéro vaut demande de résiliation du contrat souscrit par l'Abonné auprès de l'Opérateur Donneur. Cette résiliation s'applique à tous les services associés souscrits par l'Abonné auprès de l'Opérateur Donneur ;

- la résiliation du contrat avec l'Opérateur Donneur prend effet avec le Portage effectif du Numéro, sans préjudice, le cas échéant, des dispositions contractuelles relatives aux durées minimales d'engagement ;

- la date et la plage horaire prévues pour le Portage effectif du Numéro Mobile qui intervient. sauf demande expresse de l'Abonné Mobile dans un délai maximum de 2 jours ouvrables, sous réserve de la disponibilité de l'accès et sous réserve de la purge de tout délai de rétractation ou de renonciation.

13.4. L'Abonné Mobile mandate l'Opérateur Receveur pour effectuer l'ensemble des actes nécessaires à la réalisation de la Portabilité.

13.5. L'Opérateur Receveur se charge alors, pour le compte de l'Abonné Mobile de réaliser auprès de l'Opérateur Donneur et, le cas échéant des autres Opérateurs, l'ensemble des modalités de mise en œuvre de sa Demande de Portage et, de la résiliation de son contrat avec l'Opérateur Donneur.

13.6. L'Opérateur Receveur envoie la Demande de Portage à l'Opérateur Donneur. Ce dernier vérifie si le numéro est actif au jour du Portage et si les conditions d'éligibilité de cette demande sont acquises et notamment que les informations requises y figurent.

L'Opérateur Donneur ne peut refuser la Demande de Portage présentée par l'Opérateur Receveur au nom de l'Abonné Mobile que dans les cas suivants :

- Données incomplètes ou erronées : la Demande de Portage doit notamment comporter le Numéro Mobile objet de la demande et le relevé d'identité opérateur mobile (RIO mobile) correspondant ;

- Numéro Mobile inactif au jour du Portage ;

- Numéro Mobile faisant déjà l'objet d'une Demande de Portage non encore exécutée;

- Numéro de Mobile ayant déjà fait l'objet d'une Demande de Portage il y a moins de 90 jours.

13.7. L'Opérateur Donneur notifie toute non-conformité à l'Opérateur Receveur en y joignant tout détail utile. Ce dernier informe l'Abonné Mobile de la non-conformité dans les meilleurs délais et, le cas échéant des mesures correctives.

La Demande de Portage ainsi que le contrat souscrit auprès de l'Opérateur Receveur est annulée. Le contrat avec l'Opérateur Donneur est maintenu.

Seul l'Opérateur Receveur peut annuler une Demande de Portage auprès de «Opérateur Donneur. L'annulation n'est valable que si elle est adressée par «Abonné Mobile à l'Opérateur Receveur au plus tard le jour ouvrable avant la date prévue du Portage.

Avant de prendre en compte cette demande d'annulation, l'Opérateur Receveur informe l'Abonné Mobile des conséquences contractuelle de cette annulation.

13.8. Si les conditions d'éligibilité sont remplies, la Demande de Portage est validée par l'Opérateur Donneur qui notifie l'éligibilité à l'Opérateur Receveur afin de finaliser le traitement de la demande.

13.9. L'Abonné Mobile est informé de l'avancée du traitement de sa Demande de Portage par la réception de plusieurs SMS conformes aux modèles joints en Annexé 1, notamment :

- L'Opérateur Donneur lui confirme la prise en compte de sa Demande de conservation du Numéro Mobile et de résiliation du contrat dès le retour d'éligibilité ;

- L'Opérateur Receveur lui confirme la date et la plage horaire du portage la veille ou le matin du jour du Portage ;

- L'Opérateur Receveur lui confirme le Portage dès qu'il est effectif.

13.10. Dans le cadre du traitement d'une Demande de Portage, une interruption de service est tolérée le jour du Portage. Elle correspond à la période de temps durant laquelle l'Abonné Mobile ne dispose pas de l'ensemble de ses services entrants et sortants de communication mobile ni auprès de l'Opérateur Donneur, ni auprès de l'Opérateur Receveur. Cette interruption de services ne peut dépasser 6 heures et ne peut avoir lieu que le jour du Portage.

13.11. A la date de réalisation du Portage, l'abonné mobile change sa carte « SIM » et peut bénéficier des services de l'Opérateur Receveur. Tant que le Portage. effectif du numéro mobile n'a pas été réalisé, l'Opérateur Donneur ne peut utiliser les données du Serveur d'Information, ni celles d'une Demande de Portage pour

informer ses services commerciaux de la demande en cours et de la résiliation du contrat de l'Abonné Mobile.

Art. 14 : Protocole commun et autres spécifications

Dans le cadre d'une Demande de Portage et de l'utilisation d'un Numéro porté, les Opérateurs concernés doivent nécessairement communiquer selon un protocole commun dont l'objet est de permettre la réalisation du Portage et l'utilisation du Numéro Porté, s'agissant notamment du routage des communications.

Les spécifications de ce protocole commun ainsi que toute spécifications portant sur des éléments opérationnels ayant un caractère commun aux Opérateurs seront établies par l'ARCEP et entreront en vigueur par voie de décision de l'ARCEP.

CHAPITRE IV : QUALITE DE SERVICE

Art. 15 : Information des Abonnés

Le Serveur d'Information sur le Portage mis en place par chaque Opérateur Mobile est accessible gratuitement et pleinement fonctionnel 7j /7 et 24h/24.

Lorsqu'un Abonné Mobile le consulte pour obtenir des informations sur le Portage de son Numéro Mobile, le retour d'information se fait par SMS et doit intervenir dans les deux minutes qui suivent l'appel du demandeur dans 90 % des cas et dans les cinq minutes dans 99 % des cas.

Les Opérateurs Mobiles mettent en place des mécanismes de suivi de la disponibilité du Serveur d'Information afin de produire notamment les indicateurs suivants :

- Volume d'appels ;
- Taux de disponibilité ;
- Volume de SMS ;
- Pourcentage de SMS envoyés dans le 2 minutes ;
- Pourcentage de SMS envoyés entre 2 et 5 minutes ;
- Pourcentage de SMS envoyés dans les 5 minutes.

Art. 16 : Délais inter-Opérateurs de traitement de la Demande de Portage

Les demandes de Portage acceptées par l'Opérateur Receveur, sont transmises à l'Opérateur Donneur dans les meilleurs délais et au maximum :

- Pour les délais de Portage inférieur ou égaux à trois jours ouvrables : le jour même dans 80 % des cas et au plus tard le lendemain avant 12 heures.
- Pour les délais de Portage supérieurs à trois jours ouvrables: le lendemain dans 80% des cas et au plus tard le surlendemain avant 12 heures.

Après réception de la Demande de Portage, l'Opérateur Donneur confirme l'éligibilité à l'Opérateur Receveur dans les meilleurs délais et au maximum le lendemain dans 80 % des cas et au plus tard le surlendemain à 12 heures.

Le Portage effectif du Numéro Mobile doit être réalisé au plus tard un jour ouvrable après confirmation de l'éligibilité par l'Opérateur Donneur, sous réserve que l'Abonné Mobile n'ait pas expressément demandé une mise en œuvre du Portage à une date ultérieure.

Art. 17 : Qualité de service relatives à l'acheminement des communications à destination des Numéros Portés

L'interruption de service, en émission ou en réception, subie par l'Abonné Mobile au jour effectif du Portage ne peut être supérieure à 6 heures.

Sous réserve de cette seule tolérance, l'acheminement des communications à destination des Numéros Mobiles Portés se fait dans des conditions de qualité de service identiques à celle à destination des Numéros Mobiles non portés.

Art. 18 : Suivi des réclamations

Les Opérateurs fournissent, à la demande de l'ARCEP, les données statistiques relatives au nombre de réclamations reçues concernant respectivement les retards, l'inexécution ou ta mauvaise exécution des demandes de Portage ainsi que les mesures correctives prises par l'Opérateur concerné et le délai de mise en œuvre desdites mesures.

Art. 19 : Transmission des indicateurs et données à l'ARCEP

Tous les indicateurs et données spécifiés à la présente Décision sont suivis par les Opérateurs par des moyens applicatifs appropriés et sont communiqués, de même que les données brutes qui ont permis de les établir, sans délai à l'ARCEP à sa demande, sous le format requis par l'ARCEP.

Art. 20 : Entrée en vigueur

La présente décision prend effet à compter de sa date d'homologation par arrêté.

Fait à Lomé, le 18 juillet 2022

Le Directeur général

Michel Yaovi GALLEY

ANNEXE :

1. Spécifications relatives au RIO Mobile

Le RIO Mobile est constitué de quatre champs suivant la structure suivante *« OO Q RRRRRR CCC »* dans laquelle :

- **Champ *« OO »*** : champ codé sur deux caractères numériques identifiant J'Opérateur Donneur ;
- **Champ «Q»** : champ codé sur un caractère alphanumérique correspondant à la qualité de l'abonné mobile. Ce champ peut prendre deux modalités « P » pour « particulier » ou « E » pour « Entreprise » ;
- **Champ « RRRRRR »** : champ codé sur six caractères alphanumériques constituant une référence du contrat associé au numéro mobile pour J'Opérateur Donneur ;
- **Champ « CCC »** : champ codé sur trois caractères alphanumériques constituant une clé permettant de vérifier la cohérence entre le numéro mobile de l'abonné mobile et les trois premiers champs du RIO Mobile.

2. Messages transmis à l'Abonné Mobile par les Opérateurs Mobiles lors du traitement de la Demande de Portage

✓ **SMS n° 1** : Information de l'Abonné Mobile sur sa situation auprès de l'Opérateur Donneur et communication du RIO
L'Opérateur Donneur envoie à l'Abonné Mobile une série de SMS comportant de manière claire et intelligibles les messages suivants :

• ***« [Nom] [Prénom] est titulaire d'un contrat. Le RIO est : [OO Q RRRRRR CCC] »***

• ***« Le solde total de votre crédit est [à compléter]. Votre crédit expire le [à compléter] »***

• ***« Le solde de votre forfait est [à compléter forfait par forfait]. Votre forfait [o] expire le [à compléter forfait par forfait] »***

• ***« Le solde de votre porte-monnaie électronique est de [à compléter]. Il expire le [à compléter] »***

Lorsqu'il existe un engagement non échu à la date d'interrogation du Serveur d'Information par l'Abonné Mobile : ***« L'engagement de [Nom] [Prénom] contracté le [JJ/MM/AAAA1] prendra fin le [JJ/MM/AAAA2]. Le RIO est : [OO Q RRRRRR CCC]. »*** **;**

✓ **SMS n° 2** : Confirmation de la programmation du Portage
Après confirmation de l'éligibilité au Portage par l'Opérateur Receveur, l'Opérateur Donneur envoie à l'Abonné Mobile le message suivant :

« Conformément à votre demande, la résiliation avec portabilité du numéro [9XXXXXXX] sera effectuée le [JJ/MM/AAAA) entre [Heure début] et [Heure fin] ».

✓ **SMS n° 3** : Confirmation du Portage par l'Opérateur Receveur

L'Opérateur Receveur envoie à l'Abonne Mobile la veille ou le matin du Portage le message suivant :

« Conformément à votre demande, la portabilité de votre numéro [9XXXXXXX] sera effectuée vers [Dénomination commerciale de l'Opérateur] le [JJ/MM/AAAA] entre [Heure début] et [Heure fin]. »

✓ **SMS n° 4** : Annulation d'une Demande de Portage à la suite d'une demande de l'Abonné Mobile

L'opérateur Receveur envoie à l'Abonné Mobile à la suite de la prise en compte de sa demande d'annulation le message suivant :

« Conformément à votre demande, la portabilité de votre numéro [9XXXXXXX] vers [Dénomination commerciale de l'opérateur] a été annulée. Pour plus d'informations contacter le service client au [compléter avec le numéro du service client]. »

✓ **SMS n° 5** : Annulation d'une Demande de Portage en cas de non-éligibilité

L'Opérateur Receveur envoie à l'Abonné Mobile le message suivant :

« La portabilité du [9XXXXXXX] vers [Dénomination commerciale de l'Opérateur a été annulée pour une raison technique. Pour plus d'informations appeler le service client au [compléter avec le numéro du service client]. »

✓ **SMS n° 6** : Message de bienvenue en cas de Portabilité effective.

L'Opérateur Receveur envoie à l'Abonné Mobile un message de bienvenue.

Imp. Editogo
Dépôt légal n° 31 ter