AMABWIRIZA Nº 010/R/CR-CSI /RURA/020 YO KU WA 29/5/2020 AGENGA UMUTEKANO W'URUSOBE KORANABUHANGA

REGULATION Nº 010/R/CR-CSI/RURA/020 OF 29/05/2020 GOVERNING CYBERSECURITY

REGLEMENT Nº 010/R/CR-CSI/RURA/020 DU 29/05/2020 RELATIF A LA CYBERSECURITE

ISHAKIRO

TABLE OF CONTENTS

TABLE DES MATIERES

UMUTWE WA III: IGENZURA RY'UMUTEKANO HAGAMIJWE KURINDA UMUYOBORO N'URUSOBE KORANABUHANGA BY'ABAHAWE IMPUSHYA N'AMAKURU Y'ABAFATABUGUZI	**CHAPTER III: SECURITY CONTROLS TO PROTECT THE NETWORK AND SYSTEMS OF LICENSEES AND SUBSCRIBER'S INFORMATION**	**CHAPITRE III : CONTROLES DE SECURITE AFIN DE PROTEGER LE RESEAU ET LES SYSTEMES DES TITULAIRES DE LICENCES ET LES INFORMATIONS DES ABONNES**
Ingingo ya 7: Ingamba z'umutekano	**Article 7: Security Measures**	**Article 7: Mesures de sécurité**
Ingingo ya 8: Igenzura ry'umutekano rikwiye	**Article 8: Appropriate Security Controls**	**Article 8: Contrôles appropriés de sécurité**
Ingingo ya 9: Gushyira ibice mu miyoboro	**Article 9: Establishment of Layers in Network Facilities**	**Article 9: Etablissement des couches dans les installations des réseaux**
Ingingo ya 10: Akamaro k'ibice mu miyoboro	**Article 10: Importance of Layers in the Network facilities**	**Article 10: Importance des couches dans les installations de réseau**
Ingingo ya 11: Kurinda igice cy'imicungire	**Article 11: Protection of the Management Plane**	**Article 11: Protection de la couche de gestion**
Ingingo ya 12: Kurinda igice cy'igenzura	**Article 12: Protection of the Signalling or Control Plane**	**Article 12: Protection du plan de signalisation ou de commande**
Ingingo ya 13: Kurinda igice cy'amakuru	**Article 13: Protection of the data plane**	**Article 13: Protection de la couche des données**
Ingingo ya 14: Iby'ingenzi bisabwa mu igenzura ry'igice cy'amakuru	**Article 14: Required Minimum Controls for Data Plane**	**Article 14: Contrôles minimaux requis pour la couche des données**
Ingingo ya 15: Imicungire n'irindwa ry'imiyoboro n'urusobe koranabuhanga	**Article 15: Management and Protection of Networks and Systems**	**Article 15: Gestion et protection des réseaux et des systèmes**

Ingingo ya 16: Amakuru yerekeye nomero ya telefoni ihamagaye	**Article 16: Call ID Information**	**Article 16: Information d'identification de l'appel**
Ingingo ya 17: Kwegurira undi muntu urusobe n'ibikorwa koranabuhanga	**Article 17: Outsourcing Systems and Operations to a Third Party**	**Article 17: Externalisation des systèmes et des opérations à un tiers**
Ingingo ya 18: Ibisabwa mu kwegurira undi muntu urusobe n'ibikorwa koranabuhanga	**Article 18: Conditions of Outsourcing the System and Operations to a Third Party**	**Article 18: Conditions d'externalisation du système et des opérations à un tiers**
Ingingo ya 19: Inzira zikurikizwa mu gusaba uburenganzira	**Article 19: Authorization Procedures**	**Article 19: Procédures d'autorisation**
UMUTWE WA IV: ISUZUMA RY'UMUTEKANO N'UBUGENZUZI BW'IMIYOBORO N'URUSOBE KORANABUHANGA BY'UWAHAWE URUHUSHYA	**CHAPTER IV: SECURITY ASSESSEMENT AND AUDIT OF NETWORKS AND SYSTEMS OF LICENSEES**	**CHAPITRE IV: EVALUATION DE LA SECURITE ET AUDIT DES RESEAUX ET DES SYSTEMES DES TITULAIRES DE LICENCE**
Ingingo ya 20: Isuzuma ry'umutekano w'ibice byose	**Article 20: Security Assessment of All Planes**	**Article 20: Evaluation de la sécurité de toutes les couches**
Ingingo ya 21: Isuzuma ryo kureba ahashobora kwibasirwa	**Article 21: Vulnerability Assessment**	**Article 21: Evaluation de la vulnérabilité**
Ingingo ya 22: Ubugenzuzi bw'imbere	**Article 22: Internal Audit**	**Article 22: Audit interne**
Ingingo ya 23: Igenzura nzibacyuho	**Article 23: Compensatory Controls**	**Article 23: Contrôles compensatoires**
Ingingo ya 24: Koroshya ibibazo byatuma abafatabuguzi babura serivisi	**Article 24: Mitigation of risks leading to subscribers' loss of service**	**Article 24: Atténuation des risques entraînant la perte de service des abonnés**
Ingingo ya 25: Itangwa rya raporo y'isuzuma ry'umutekano n'iy'ubugenzuzi	**Article 25: Submission of the Security Assessment and Audit Report**	**Article 25: Présentation de rapport d'évaluation de sécurité et d'audit**

AMABWIRIZA Nº 001/R/CSSI/RURA/020 YO KU WA …/…/2020 AGENGA UMUTEKANO W'URUSOBE KORANABUHANGA	**REGULATION GOVERNING CYBERSECURITY Nº 001/R/CSSI/RURA/020 OF …/…/2020**	**REGLEMENT N^{O} 001/R/CSSI/RURA/020 DU …/…/2020 RELATIF A LA CYBERSECURITE**
Inama Ngenzuramikorere	**The Regulatory Board**	**Le Conseil de Régulation**
Ishingiye ku Itegeko n° 04/2013 ryo ku wa 08/02/2013 ryerekeye kubona amakuru mu Rwanda cyane cyane mu ngingo yaryo ya 4;	Pursuant to law n° 04/2013 of 08/02/2013 relating to access to information in Rwanda especially in Article 4;	Vu la Loi n° 04/2013 du 08/02/2013 relative à l'accès à l'information au Rwanda, spécialement en son article 4 ;
Ishingiye ku Itegeko n° 60/2013 ryo ku wa 22/08/2013 rigena igenzura ry'itumanaho cyane cyane mu ngingo yaryo ya 5;	Pursuant to law n° 60/2013 of 22/08/2013 regulating the Interception of Communications especially in Article 5;	Vu la Loi n° 60/2013 du 22/08/2013 réglementant l'interception des communications spécialement en son article 5;
Ishingiye ku Itegeko n° 09/2013 ryo ku wa 01/03/2013 rishyiraho Urwego rw'Igihugu rushinzwe kugenzura imikorere y'inzego zimwe z'imirimo ifitiye Igihugu akamaro (RURA) rikanagena inshingano, ububasha, imiterere, n'imikorere byarwo, cyane cyane mu ngingo yaryo ya 2;	Pursuant to law n° 09/2013 of 01/03/2013 establishing Rwanda Utilities Regulatory Authority (RURA) and determining its mission, powers, organization and functioning**,** especially in Article 2;	Vu la Loi n° 09/2013 du 01/03/2013 portant création de l'Autorité Rwandaise de Régulation de certains services d'utilité publique (RURA) et déterminant sa mission, ses pouvoirs, son organisation et son fonctionnement, spécialement en son article 2 ;
Ishingiye ku Itegeko n° 24/2016 ryo ku wa 18/06/2016 rigenga ikoranabuhanga mu itangazabumenyi n'itumanaho, cyane cyane mu ngingo zaryo iya 123, iya 124, iya 125, iya 126 n'iya 127;	Pursuant to law n° 24/2016 of 18/06/2016 governing information and communication technologies especially in Articles 123, 124, 125, 126 and 127;	Vu la Loi n° 24/2016 du 18/06/2016 régissant les technologies de l'information et de la communication, spécialement en ses articles 123, 124, 125, 126 et 127 ;

Ishingiye ku Itegeko nº 60/2018 ryo ku wa 22/8/2018 ryerekeye gukumira no guhana ibyaha bikoreshejwe ikoranabuhanga;

Pursuant to Law Nº 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes;

Vu la Loi nº 60/2018 du 22/8/2018 portant prévention et répression de la cybercriminalité ;

Ishingiye ku Iteka rya Minisitiri w'Intebe n° 90/03 ryo ku wa 11/09/2014 rigena uburyo itegeko ryerekeye igenzura ry'itumanaho rishyirwa mu bikorwa, cyane cyane mu ngingo zaryo iya 8 n'iya 9;

Pursuant to the Prime Minister's Order n° 90/03 of 11/09/2014 determining modalities for the enforcement of the law regulating interception of communication especially in Articles 8 and 9;

Vu l'Arrêté du Premier Ministre n° 90/03 du 11/09/2014 portant modalités d'exécution de la loi règlementant l'interception des communications, spécialement en ses articles 8 et 9 ;

Ishingiye ku myanzuro y'inama nyunguranabitekerezo n'abafatanyabikorwa yabaye ku wa 2 Ukwakira 2019;

Considering deliberations from the consultative meeting held on October 2nd, 2019 with stakeholders;

Suite aux délibérations de la réunion consultative tenue le 2 octobre 2019 avec les parties prenantes ;

Imaze kuyasuzuma no guyafataho umwanzuro mu nama yayo yo ku wa 29 Gicurasi 2020 ;

Upon due consideration and deliberation in its meeting of May 29th, 2020;

Après examen et délibération en sa séance du 29 Mai, 2020 ;

ISHYIZEHO amabwiriza akurikira:

HEREBY issues the following Regulation;

EDICTE le règlement suivant :

UMUTWE WA MBERE: INGINGO RUSANGE

CHAPTER ONE: GENERAL PROVISIONS

CHAPITRE PREMIER : DISPOSITIONS GENERALES

Ingingo ya mbere: Icyo aya mabwiriza agamije

Aya mabwiriza agamije kubungabunga umutekano w'imiyoboro, uw'abafatabuguzi n'uw'ibikorwaremezo by'ikoranabuhanga byihariye mu rwego rwo kurinda ubuzima bwite, umwimerere no gufata neza imiyoboro n'urusobe rw'ikoranabuhanga mu Rwanda.

Article One: Purpose of this Regulation

The purpose of this Regulation is to secure networks, their subscribers and the critical communication infrastructure to ensure the confidentiality, integrity and availability of networks and systems in Rwanda.

Article premier : Objet du présent règlement

Le présent règlement a pour objet de garantir la sécurité des réseaux, leurs abonnés et de l'infrastructure de communication importante en vue d'assurer la confidentialité, l'intégrité et la disponibilité des réseaux et des systèmes informatiques au Rwanda.

Ingingo ya 2: Ibisobanuro by'amagambo

Muri aya mabwiriza, amagambo akurikira afite ibisobanuro bikurikira:

1. **Abatanga serivisi zifatiye ku itumanaho**: uwahawe uruhushya rwo guha abafatabuguzi ubwoko bwose bwa serivisi zifatiye ku itumanaho akoresheje ibikorwa remezo by'abandi bantu bafite impushya zo gutanga serivisi z'imiyoboro;

2. **Umwirondoro w'uhamagaye**: serivisi iba muri telefoni za kera n'izikoresha imibare, yohereza telefoni y'uhamagawe nimero y'umuhamagaye n'izina ryanditse kuri iyo nimero ihamagaye mu gihe telefoni iri gusohora ijwi, cyangwa mu gihe ihamagara ririmo rikorwa ariko ritaritabwa;

3. **Ubugenzuzi ry'ubahirizwa ry'ibisabwa**: isuzuma ryimbitse rigamije kureba ko umuryango uyu n'uyu wubahiriza ibikubiye muri aya mabwiriza;

4. **Ikibazo gikomeye**: ikibazo gituma abakiriya babura serivisi z'ibanze kandi kikagira ingaruka no ku bindi bifatiye kuri izo serivisi ku buryo bwose,

Article 2: Definitions of terms

For the purpose of this Regulation, terms below shall have the following meanings:

1. **Application Service Provider**: any licensed operator offering all forms of ICT applications to end users by using the infrastructure of other licensed Network Service Providers;

2. **Caller Identification:** a telephone service, available in analogue and digital phone systems, that transmits a caller's number and the name associated with the calling telephone number where possible to the called party's telephone equipment during the ringing signal, or when the call is being set up but before the call is answered;

3. **Compliance Audit**: a comprehensive review of an organization's adherence to this regulation

4. **Critical Incident:** An incident that results in critical loss of core service and entirely affects value-added services;

Article 2 : Définitions des termes

Aux fins du présent règlement, les termes suivants ont les significations suivantes :

1. **Fournisseur des services d'application** : tout opérateur agréé offrant toutes les formes d'applications de ICT aux utilisateurs finaux en utilisant l'infrastructure des autres fournisseurs de services réseau agréés ;

2. **Identification de l'appelant** : service téléphonique, disponible dans les systèmes téléphoniques analogues et numériques, qui transmet si possible le numéro de l'appelant et le nom associé au numéro de téléphone appelant à l'équipement téléphonique de l'appelé pendant la sonnerie ou lors de l'établissement de l'appel mais avant de répondre à l'appel ;

3. **Audit de conformité** : examen complet de l'adhésion d'une organisation à ce règlement ;

4. **Incident critique** : incident qui entraîne une perte critique de service de base et qui affecte entièrement la valeur ajoutée des services ;

5. **Amakuru yihariye y'umufatabuguzi**: amakuru ayo ari yo yose aturutse mu guhamagara, kohereza ubutumwa bugufi n'ibikorwa byakozwe nk'ububiko bw'amajwi, serivisi z'imari zikorewe kuri telefoni ngendanwa cyangwa ibijyanye n'inyemezabuguzi n'ubutumwa bugufi;

6. **Amakuru**: amakuru uko yaba ateye kose aboneka hakoreshejwe ikoranabuhanga;

7. **Ikimenyetso koranabuhanga**: ibikorwa n'amakuru koranabuhanga by'umuntu ku giti cye bishobora kugaragazwa kuri murandasi cyangwa ku kindi gikoresho koranabuhanga;

8. **Ubugenzuzi bwigenga ku mutekano**: isuzuma ryimbitse rikorwa n'urwego rwo hanze rubyemerewe, kugira ngo hasuzumwe uko umutekano w'amakuru uhagaze mu bikorwa by'uwahawe uruhushya no kugira ngo hateganywe ingamba zo gukaza umutekano;

9. **Umutekano w'amakuru**: igikorwa kibuza ko amakuru agerwaho, akoreshwa, atangazwa, arogowa, ahindurwa, asomwa, agenzurwa, abikwa cyangwa yangizwa mu buryo butemewe;

5. **Subscriber Personal Information:** any information generated through regular calls, SMS and transactions history such as Call data record, mobile financial services or Billing record and SMS details;

6. **Data:** Electronic representations of information in any form;

7. **Digital Footprint:** refers to one's unique set of traceable digital activities, actions, contributions and communications that are manifested on the Internet or on digital devices;

8. **Independent security Audit**: a comprehensive assessment conducted by external party, which is allowed, in order to assess the current condition of Information Security in the business of the licensee and to plan timely actions in order to increase the level of security.

9. **Information Security:** The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction;

5. **Informations personnelles de l'abonné** : toute information générée par les appels réguliers, les SMS et l'historique des transactions, telles que l'enregistrement des données d'appel, les services financiers mobiles ou le relevé de facturation et les détails de SMS ;

6. **Données** : representations électroniques d'information sous quelle forme que ce soit;

7. **Empreinte numérique** : gamme unique d'activités, d'actions, de contributions et de communications numériques traçables qui se manifestent sur internet ou sur des appareils numériques ;

8. **Audit de sécurité indépendant** : évaluation complète réalisée par une partie externe qui est autorisée, afin d'évaluer l'état actuel de la sécurité de l'information dans l'entreprise du titulaire de licence et de planifier des actions en temps opportun afin d'augmenter le niveau de sécurité ;

9. **Sécurité de l'information** : pratique consistant à protéger les informations contre tout accès, utilisation, divulgation, perturbation, modification, lecture, inspection, enregistrement ou destruction non autorisés ;

10. **Ibikorwa remezo na serivisi**: amakuru, uburyo, ibikoresho, imiyoboro na porogaramu koranabuhanga;
11. **ISO/IEC**: komite ishinzwe ibya tekiniki ihuriweho n'Ikigo Mpuzamahanga cy'Ubuziranenge (ISO) na Komisiyo Mpuzamahanga Ishinzwe iby'Ikoranabuhanga (IEC). Intego yayo ni ugushyiraho, kwita no guteza imbere ubuziranenge mu bijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;
12. **IT**: ikoranabuhanga mu itangazabumenyi;
13. **KPI**: igipimo nsuzumabikorwa ni igipimo gikoreswa mu gusuzuma ibintu by'ingenzi byatumye umuryango uyu n'uyu cyangwa serivisi yatanzwe byarageze ku musaruro;
14. **Uwahawe uruhushya rwo gutanga serivisi za murandasi**: isosiyete ifite uruhushya rwo kudandaza serivisi za murandasi ikazigeza kuri rubanda, cyangwa ibikorwa by'ubucuruzi n'indi miryango;
15. **Uwahawe uruhushya rwo gutanga serivisi z'itumanaho**: umuntu utanga serivisi z'itumanaho ufite uruhushya rwatanzwe n'Urwego Ngenzuramikorere;
16. **Uwahawe uruhushya**: umuntu ufite uruhushya rwatanzwe n'Urwego Ngenzuramikorere hakurikijwe aya mabwiriza;

10. **Infrastructure and services**: Include data, system, equipment, networks and applications;
11. **ISO/IEC**: is a joint technical committee of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Its purpose is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT);
12. **IT:** Information Technology;
13. **KPI:** A key performance indicator (KPI) is a business metric used to evaluate factors that are crucial to the success of an organization or service provided;
14. **Licensed Internet Service Provider:** A licensed company that provides retail access to the Internet for members of the public, or for businesses and other organizations;
15. **Licensed Telecom Operator:** A Telecommunication Service provider holding a valid License issued by the Regulatory Authority;
16. **Licensee:** a person who holds a license issued by the Regulatory Authority under this regulation;

10. **Infrastructures et services**: données, systèmes, équipements, réseaux et applications ;
11. **ISO/CEI**: comité technique conjoint de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI). Son objectif est d'élaborer, de maintenir et de promouvoir les normes dans les domaines des technologies de l'information (TI) et des technologies de l'information et de la communication (TIC)
12. **TI** : technologie de l'information ;
13. **KPI**: un indicateur clé de performance (KPI) est une mesure commerciale utilisée pour évaluer les facteurs cruciaux pour le succès d'une organisation ou d'un service fourni;
14. **Fournisseur des services internet agréé**: société agréée qui fournit au détail un accès à l'internet aux membres du public ou aux entreprises et aux autres organisations ;
15. **Opérateur agrée des télécommunications** : fournisseur de services de télécommunications titulaire d'une licence valide délivrée par l'Autorité de Régulation ;
16. **Titulaire de licence** : personne titulaire d'une licence délivrée par l'Autorité de Régulation en vertu du présent règlement ;

17. **Ikibazo kinini**: ikintu gitera ibura rikomeye rya seirivisi zigerwaho hifashishijwe serivise zitangwa n'uwahawe uruhushya ;

18. **Ikibazo cyoroheje**: ikintu kigira ingaruka zoroheje ku bakiriya, kandi kikababuza kugera kuri serivisi zitangwa n'uwahawe uruhushya,

19. **Ikibazo kiringaniye**: ikintu gifite ingaruka ku gice cya serivisi z'ibanze zihabwa umufatabuguzi,
20. **Ibikoresho by'umuyoboro**: ibikoresho byose byitabazwa by'umwihariko mu miyoboro rusange y'itumanaho koranabuhanga;
21. **Abatanga serivisi z'ibikorwa remezo by'itumanaho**: abahawe uruhushya bafite, bakoresha cyangwa batanga ubwoko ubwo ari bwo bwose bw'ibikorwa remezo byifashishwa mu gutwara cyangwa gutanga serivisi n'ibikubiye muri serivisi;

22. **Abatanga serivisi z'imiyoboro**: abahawe impushya zo gutanga serivisi ku bakoresha imiyoboro y'itumanaho koranabuhanga. Barimo n'abatanga serivisi za murandasi badatunze ibikorwa remezo;

23. **Uburyo bw'imicungire y'umuyoboro (NMS)**: uruhererekane rw'ibikoresho na porogaramu bya mudasobwa bifasha

17. **Major Incident:** An event that causes significant loss of value-added service;

18. **Minor Incident:** event that has impact on some customers, and limits their access to value-added services;

19. **Moderate Incident:** An event that has a partial impact on core services of the subscriber;
20. **Network Facilities:** Any elements used in connection with the provision of public electronic communication networks;
21. **Network Infrastructure Service Providers**: Licensees who own, operate or provide any form of active or passive physical infrastructure used for carrying or providing services, applications and content;

22. **Network Service Providers:** Licensees who provide services to those using electronic communications networks**.** These include Internet Service Providers who do not own infrastructure;

23. **Network Management System (NMS):** A set of hardware and/or software tools that allow an IT professional to supervise

17. **Incident majeur** : événement qui entraîne une perte significative des services à valeur-ajoutée ;

18. **Incident mineur** : événement qui a un impact sur les clients, et qui limite leur accès aux services à valeur ajoutée ;

19. **Incident modéré** : événement qui a un impact partiel sur les services de base de l'abonné ;
20. **Installations du réseau** : tous les éléments utilisés principalement en relation avec la fourniture de réseaux de communication électronique publics ;
21. **Fournisseurs des services d'infrastructures de réseau** : titulaires des licences qui possèdent, opèrent ou fournissent toute forme d'infrastructure physique active ou passive utilisée pour transporter ou fournir des services, des applications et du contenu ;

22. **Fournisseurs des services réseau** : titulaires de licence fournisseurs de services aux utilisateurs des réseaux de communications électroniques. Il s'agit des fournisseurs des services internet qui ne possèdent pas d'infrastructures ;

23. **Système de gestion du réseau (NMS)** : ensemble d'outils matériels et/ou logiciels permettant à un professionnel de

inzobere mu ikoranabuhanga kugenzura ibice by'umuyoboro runaka mu micungire y'umuyoboro mugari;

24. **Amakuru bwite y'umuntu:** amakuru ayo ari yo yose yerekeye nyir'ubwite uzwi cyangwa ushobora kumenyekana hifashishijwe nomero iyo ari yo yose y'ibimuranga cyangwa ibimuranga ku mubiri, ku miterere y'ubuzima bwe, imyitwarire, ubukungu, mu mico no mu mibanire ye n'abandi;
25. **Ibikorwa remezo by'urufunguzo rusange (PKI)**: urusobe rw'ibintu bikoreshwa n'utanga serivisi y'icyemezo mu micungire y'icyemezo, imicungire y'ububiko, imicungire y'urufunguzo hakoreshejwe uburyo budasubirwamo bw'imfunguzo ebyiri;
26. **Urwego Ngenzuramikorere**: Urwego rw'Igihugu rushinzwe kugenzura imikorere y'inzego zimwe z'imirimo ifitiye Igihugu akamaro;
27. **Ikibazo cy'umutekano**: igikorwa cyose, cyaba cyagenze neza cyangwa kitagenze neza, kigamije kugera mu buryo butemewe, kurogoya cyangwa gukoresha nabi urusobe koranabuhanga cyangwa amakuru arubitsemo;

the individual components of a network within a larger network management framework;

24. **Personal data:** Any information relating to an identified or identifiable individual by reference to any number of his/her identifications or to his or her physical, physiological, mental, economic, cultural or social identity;
25. **Public Key Infrastructure (PKI):** A system of Certification Service Provider that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography;
26. **Regulatory Authority:** Rwanda Utilities Regulatory Authority;
27. **Security incident:** any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

l'informatique de superviser les différents éléments d'un réseau dans un cadre de gestion d'un réseau plus large ;

24. **Données à caractère personnel** : information relative à une personne physique identifiée ou qui peut être identifiée par référence à tout numéro de son identification ou à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;
25. **Infrastructure à clé publique (PKI)**: système de fournisseur des services de certification qui effectue un ensemble de fonctions de gestion de certificats, de gestion d'archives, de gestion de clés et de gestion du code d'accès pour une communauté d'utilisateurs dans une application de cryptographie asymétrique ;
26. **Autorité de Régulation** : Autorité Rwandaise de Régulation de certains services d'utilité publique ;
27. **Incident de sécurité** : tout acte ou tentative, réussi ou échoué, d'obtenir un accès non autorisé, de perturber ou d'abuser le système d'information ou des informations stockées sur ce système d'information.

28. **Amasezerano ashingiye ku mitangire ya serivisi (SLA)**: igice cy'amasezerano ya serivisi, aho serivisi isobanurwa birambuye. Iby'ingenzi mu bigize serivisi – aho serivisi igarukira, ubwiza bwayo, inshingano – byumvikanwaho hagati y'utanga serivisi n'uyikoresha;
29. **Ubutumwa bugufi (SMS)**: serivisi y'ubutumwa bugufi kuri telefoni, murandasi cyangwa uburyo bw'itumanaho rigendanwa, ikoresha amasezerano y'itumanaho yemewe kugira ngo telefoni zitagendanwa cyangwa izigendanwa zibashe guhererekanya ubutumwa bugufi;
30. **Umuyoboro ngenzuzi**: igice cy'umuyoboro w'itumanaho koranabuhanga gikoreshwa mu gutumanaho hagati y'urusobe koranabuhanga, abafatabuguzi n'abatanga serivisi;
31. **Umufatabuguzi**: umuntu wese ufitanye amasezerano n'utanga serivisi z'itumanaho rusange rikoresha ikoranabuhanga kugira ngo ahabwe izo serivisi.
32. **Ibipimo ngenderwaho**: ibipimo ngenderwaho bivuga amabwiriza mpuzamahanga nka ISMS ISO/IEC 27001: 2013 cyangwa ISO/IEC 27011 ashobora kuvugururwa;

28. **Service-Level Agreement (SLA):** A part of a service contract, where a service is formally defined. Particular aspects of the service – scope, quality, responsibilities - are agreed between the service provider and the service user;
29. **Short Message Service (SMS):** A text messaging service component of phone, Web, or mobile communication systems, which uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages;
30. **Signalling/Control plane:** a layer where specific communication protocols are used to establish calls and sessions between systems, subscribers and service providers;
31. **Subscriber:** Any person who is a party to a contract with a provider of public electronic communications services for the supply of such services.
32. **Standards:** standards refer to required international standards such as ISMS ISO/IEC 27001: 2013 or ISO/IEC 27011 as it may be amended from time to time;

28. **Accord de niveau de service (SLA)**: partie d'un contrat de service dans laquelle un service est officiellement défini. Des aspects particuliers du service – étendue, qualité, responsabilités – sont convenus entre le fournisseur des services et l'utilisateur des services ;
29. **Service de messagerie (SMS)** : composant des services de messagerie texte des systèmes de communication téléphonique, Web ou mobile, qui utilise des protocoles de communication normalisés pour permettre aux appareils de téléphones fixe ou mobile d'échanger des courts messages sous forme de texte ;
30. **Plan de signalisation/commande** : couche où des protocoles de communication spécifiques sont utilisés pour établir des appels et des sessions entre les systèmes, les abonnés et les fournisseurs des services ;
31. **Abonné** : personne liée par un contrat à un fournisseur des services publics de communications électroniques pour la fourniture de ces services.
32. **Normes** : les normes se réfèrent aux normes internationales requises telles que ISMS ISO/CEI 27001 : 2013 ou ISO/CEI 27011 pouvant être modifiées de temps en temps ;

33. **Urusobe koranabuhanga**: uruhererekane rw'ibigize itumanaho koranabuhanga birimo ibikoresho, porogaramu n'imiyoboro koranabuhanga bitunzwe, bigenzurwa, bikoreshwa, bikodeshwa cyangwa byisungwa n'utanga serivisi;

34. **Utanga serivisi z'itumanaho**: urwego rutanga serivisi z'itumanaho rusange rikoresha ikoranabuhanga;

35. **Undi muntu**: umuntu ku giti cye cyangwa isosiyete itanga ibicuruzwa cyangwa serivisi akabiha uwahawe uruhushya rwo gutanga servisi cyangwa akabitanga mu izina ry'uwahawe uruhushya;

36. **Amakuru anyuzwa ku muyoboro**: amakuru ayo ari yo yose akoreshwa mu kohereza ubutumwa ku muyoboro w'itumanaho koranabuhanga cyangwa yifashishwa mu gukora inyemezabuguzi y'ubwo butumwa. Ku muyoboro w'itumanaho rigendanwa, amakuru aba ari bice by'umuyoboro;

37. **Umuntu utabifitiye uburenganzira**: ni umuntu wese utemerewe kugera ku makuru y'umufatabuguzi hakurikijwe amategeko n'amabwiriza akurikizwa;

33. **System:** A set up of ICT components comprising of hardware, software and networking elements that are owned, controlled, operated, leased or otherwise relied on by the service provider;

34. **Telecommunication Service Provider:** An entity providing public electronic communications services;

35. **Third Party:** An individual or company supplying products or services to the service provider (licensee) or on the behalf of the licensee;

36. **Traffic Data:** any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication. In mobile networks, data is encapsulated in network packets;

37. **Unauthorized person:** is any person who is not authorized to access subscriber's information as required by the laws and regulations into force;

33. **Système** : ensemble des composants TIC comprenant du matériel, des logiciels et des éléments de réseau détenus, contrôlés, opérés, loués ou autrement utilisés par le fournisseur des services ;

34. **Fournisseur des services des télécommunications** : entité fournissant des services publics de communications électroniques ;

35. **Tiers** : personne physique ou morale fournissant des produits ou des services au fournisseur des services (titulaire de licence) ou au nom du titulaire de licence ;

36. **Données relatives au trafic** : toutes données traitées aux fins de l'acheminement d'une communication sur un réseau de communications électroniques ou de facturation en rapport avec cette communication. Dans les réseaux mobiles, les données sont encapsulées dans des paquets des réseaux ;

37. **Personne non autorisée** : toute personne qui n'est pas autorisée à accéder aux informations de l'abonné conformément aux lois et règlements en vigueur ;

38. **Ibibazo byihutirwa**: ibibazo bifatwa ko byihutirwa iyo byujuje kimwe muri ibi bikurikira:

(a) Ibibazo byose bigira ingaruka kugera kuri 25% by'umubare w'abafatabuguzi kuri serivise yagize ikibazo.
(b) Ibibazo byose bishobora gutuma serivise z'ibanze zibura kandi bikanagira ingaruka kuri zigerwaho hifashishijwe serivise zitangwa n'uwahawe uruhushya ;
(c) Ibibazo bituma itangazamakuru ry'imbere mu gihugu ribivugaho.
(d) Ibibazo bigira ingaruka ku kuri serivisi za Guverinema cyangwa serivise rusange.

39. **Ukoresha itumanaho**: umuntu wese ukoresha cyangwa usaba serivisi z'itumanaho rusange rikoresha ikoranabuhanga.

<u>Ingingo ya 3</u>: Ibirebwa n'aya mabwiriza

Aya mabwiriza areba ibikorwa remezo byose na serivisi zose z'ikoranabuhanga bihabwa rubanda bitanzwe n'uwahawe uruhushya rwo kubitanga.

38. **Urgent incidents:** Incidents shall be considered as "urgent" if they meet any of the following criteria:

(a) All incidents affecting services to 25% of the licenses' total number of subscribers on the affected service.
(b) All incident that results in loss of core services and affects the entire Value-Added Services;

(c)Incidents attracting national mainstream media coverage.
(d)Incidents affecting Government or Public Sector services.

39. **User:** any person using or requesting publicly available electronic communications services.

<u>Article 3:</u> Scope of this Regulation

This Regulation shall apply to all ICT infrastructure and services provided to the public by licensee.

38. **Incidents urgents** : les incidents sont considérés comme « urgents » s'ils répondent à l'un des critères suivants :

(a) Tous les incidents affectant les services jusqu'au 25% du nombre total d'abonnés sur le service affecté.

(b) Tout incident entraînant la perte de services essentiels et affectant l'ensemble des services à valeur ajoutée ;

(c) Incidents suscitant l'attention des médias nationaux.
(d) Incidents affectant des services du gouvernement ou du secteur public.

39. **Utilisateur** : toute personne utilisant ou sollicitant des services de communications électroniques accessibles au public.

<u>Article 3:</u> Champ d'application du présent règlement

Le présent règlement s'applique à toutes les infrastructures et services TIC fournis au public par le titulaire de licence.

Ingingo ya 4: Intego z'aya mabwiriza

Intego z'aya mabwiriza ni izi zikurikira:

(a) Kureba ko abahawe impushya bose hamwe n'abafatabuguzi babo bagenzurwa kandi bafite umutekano;
(b) gukora ku buryo abahawe impushya batanga serivisi zitekanye;
(c) gukurikirana no gucunga umutekano w'urusobe koranabuhanga;
(d) gukora ku buryo abahawe impushya barinda urusobe koranabuhanga n'inyungu z'abafatabuguzi;

(e) gukora ku buryo serivisi z'abahawe impushya zirindwa guhagarikwa, kwangizwa cyangwa kubuzwa gukora.

Article 4: Objectives of this Regulation

The objective of this Regulation is:

(a) to ensure that all licensees and their subscribers are under a controlled and secure environment;
(b) to ensure that the licensees deliver secured services;
(c) to deal with the monitoring and control of the security state of systems;
(d) to ensure that licensees protect their systems and subscribers' interests;

(e) to ensure that licensees' services are prevented from being interrupted, corrupted or denied.

Article 4: Objectifs du présent règlement

Le présent règlement a pour objectif de:

(a) assurer que tous les titulaires de licence et leurs abonnés se trouvent dans un environnement contrôlé et sécurisé;
(b) assurer que les titulaires de licence fournissent des services sécurisés;
(c) assurer la surveillance et le contrôle de l'état de sécurité des systèmes;
(d) veiller à ce que les titulaires de licence protègent leurs systèmes et les intérêts de leurs abonnés;

(e) veiller à ce que les services des titulaires de licence ne soient pas interrompus, corrompus ou refusés.

UMUTWE WA II: INSHINGANO Z'ABAHAWE IMPUSHYA N'IZ'ABAFATABUGUZI

Ingingo ya 5: Inshingano z'abahawe impushya

Uwahawe uruhushya afite inshingano zikurikira:

(a) gucunga umutekano w'amakuru yatawe, yabitswe, yatunganyijwe n'ayoherejwe mu miyoboro no mu rusobe koranabuhanga;

CHAPTER II: RESPONSIBILITIES OF LICENSEES AND SUBSCRIBERS

Article 5: Responsibilities of Licensees

The licensee shall have the following responsibilities:

(a) ensuring security of the information captured, stored, processed and transmitted in or through their networks and systems;

CHAPITRE II: ATTRIBUTIONS DES TITULAIRES DE LICENCE ET DES ABONNES

Article 5: Attributions des titulaires de licences

Le titulaire de licence a les attributions suivantes :

(a) assurer la sécurité des informations obtenues, stockées, traitées et transmises dans ou à travers ses réseaux et systèmes;

(b) gushyira mu bikorwa, gukora, gukomeza no gukurikirana igenzura rivugwa muri aya mabwiriza no mu mabwiriza mpuzamahanga nka ISO/IEC 27001: 2013 cyangwa ISO/IEC 27011 ashobora kuvugururwa;

(c) gushyiraho, kugaragaza no gukurikiza uburyo busobanutse kandi bwizewe;

(d) kurengera inyungu z'abafatabuguzi no gutuma bamugirira icyizere, abagezaho serivisi zizewe;

(e) gushyira mu bikorwa no guhozaho ingamba zihamye za tekiniki n'iz'ubuyobozi hagamijwe kurinda urusobe koranabuhanga na serivisi zihabwa abafatabuguzi;

(f) gukora ku buryo abafatabuguzi barindirwa umutekano mu buryo buwiye mu gihe bakoresha serivisi bahawe;

(g) kugeza ku Rwego Ngenzuramikorere ibibazo by'umutekano;

(h) kubahiriza ibiteganywa n'amategeko n'amabwiriza bivugwa muri aya mabwiriza no mu yandi mategeko mu Rwanda;

(i) gutanga inama zijyanye n'umutekano w'ikoranabuhanga ahagaragaye ibibazo mu gihe afite abafatabuguzi.

(b) implementing, operating, maintaining and monitoring the controls mentioned in this regulation and required international standards such as ISO/IEC 27001: 2013 or ISO/IEC 27011 as it may be amended from time to time;

(c) developing, documenting and following well defined secured processes;

(d) protecting subscribers' interests and gaining their confidence by providing secured systems and services;

(e) implementing and maintaining appropriate technical and organizational measures to secure systems and services provided to customers;

(f) ensure that users are adequately protected while using provided services.

(g) Reporting of security incidents to the Regulatory Authority;

(h) complying with all legal and regulatory requirements provided under this regulation and other laws in Rwanda.

(i) Issue cyber security related advisories where risks have been identified in the specific licensee has subscribers.

(b) assurer la mise en œuvre, opération, maintenance et la surveillance des contrôles mentionnés dans le présent règlement et les normes internationales requises telles que ISO/CEI 27001: 2013 ou ISO/CEI 27011, pouvant être modifiées de temps à autre;

(c) développer, documenter et suivre des processus sécurisés bien définis;

(d) protéger les intérêts des abonnés et gagner leur confiance en leur fournissant des systèmes et des services sécurisés;

(e) mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées afin de sécuriser les systèmes et services fournis aux clients;

(f) veiller à ce que les utilisateurs soient correctement protégés lorsqu'ils utilisent les services fournis.

(g) signaler les incidents de sécurité à l'Autorité de Régulation;

(h) se conformer à toutes les conditions légales et réglementaires prévues par le présent règlement et les autres lois au Rwanda.

(i) émettre des avis liés à la cyber sécurité lorsque les risques ont été identifiés dans le cas où le titulaire de licence aurait des abonnés.

Ingingo ya 6: Inshingano z'abafatabuguzi

Abafatabuguzi ba serivisi z'ikoranabuhanga bafata ingamba zirimo zimwe muri izi zikurikira:

a) kugenzura buri gihe no gukora ku buryo ibyangombwa koranabuhanga nk'ibijyanye no kwandikisha sim, pin, amagambo banga, konti bicungwa neza;

b) gukoresha porogaramu za ngombwa no kubika amakuru ku bikoresho koranabuhanga byabo;

c) kugira uburyo burinda kirogoya ibikoresho byabo aho bishoboka.

Article 6: Responsibilities of Subscribers

The subscribers using ICT services shall take actions comprising of but not limited to the following:

a) always verify and ensure that their digital credentials such as sim registration details, pin, passwords, user accounts, are safely protected;

b) apply necessary software patches and backup the data on their devices;

c) have antimalware on their devices where possible.

Article 6: Attributions des abonnés

Les abonnés utilisant les services TIC doivent entreprendre des actions suivantes, sans toutefois s'y limiter:

a) toujours vérifier et s'assurer que leurs identifiants numériques tels que l'enregistrement de la carte SIM, le code PIN, les mots de passe, les comptes d'utilisateur sont parfaitement protégés;

b) appliquer les correctifs nécessaires et sauvegarder les données sur leurs appareils;

c) avoir un logiciel anti-programme sur leurs appareils lorsque cela est possible.

UMUTWE WA III: IGENZURA RY'UMUTEKANO HAGAMIJWE KURINDA UMUYOBORO N'URUSOBE KORANABUHANGA BY'ABAHAWE IMPUSHYA N'AMAKURU Y'ABAFATABUGUZI

CHAPTER III: SECURITY CONTROLS TO PROTECT THE NETWORK AND SYSTEMS OF LICENSEES AND SUBSCRIBER'S INFORMATION

CHAPITRE III: CONTROLES DE SECURITE AFIN DE PROTEGER LE RESEAU ET LES SYSTEMES DES TITULAIRES DE LICENCES ET LES INFORMATIONS DES ABONNES

Ingingo ya 7: Ingamba z'umutekano

Uwahawe uruhushya wese agomba gufata ingamba zose za ngombwa z'umutekano kugira ngo arinde ibanga ubusugire, no kuboneka by'umuyoboro, urusobe koranabuhanga na serivisi mu gihe cyose uruhushya rugifite agaciro.

Article 7: Security Measures

Any Licensee must take all required security measures to guarantee the confidentiality, integrity and availability of their network, systems and services for the entire duration of the License.

Article 7 : Mesures de sécurité

Tout titulaire de licence doit prendre toutes les mesures nécessaires de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité de son réseau, de ses systèmes et de ses services pendant toute la durée de la licence.

Uwahawe uruhushya agomba gushyira mu bikorwa no guhozaho ingamba zihamye za tekiniki n'iz'ubuyobozi hagamijwe kurinda urusobe koranabuhanga na serivisi zihabwa abafatabuguzi. Izo ngamba zigomba gushyirwa mu bikorwa mu rwego rwo gufasha umufatabuguzi kurinda amakuru ye bwite, abashobora kuyakoresha mu buryo butemewe cyangwa se akazimira, akagerwaho cyangwa agatangazwa mu buryo bw'impanuka cyangwa bunyuranyije n'amategeko.

The Licensee is required to implement and maintain appropriate technical and organizational measures to secure systems and services provided to their subscribers. Such measures must be implemented to support customer secure personal data against unauthorized processing and accidental or unlawful loss, access or disclosure.

Le titulaire de licence est tenu de mettre en œuvre et de maintenir les mesures techniques et organisationnelles nécessaires pour sécuriser les systèmes et les services fournis à ses souscripteurs. Ces mesures doivent être mises en œuvre pour aider le client à sécuriser les données personnelles contre le traitement non autorisé et la perte accidentelle et illégale, accès ou divulgation.

Izo ngamba zigomba kuba zihamye kugira ngo zikumire cyangwa zigabanye ingaruka z'ibibazo by'umutekano ku bafatabuguzi, ku yindi miyoboro no ku rusobe koranabuhanga.

These security measures must be adequate to prevent or minimize the impact of security incidents on the subscribers, interconnected networks and systems.

Ces mesures de sécurité doivent être adéquates en vue de prévenir ou minimiser l'impact des incidents de sécurité sur les abonnés, les réseaux et les systèmes interconnectés.

<u>Ingingo ya 8</u>: Igenzura ry'umutekano rikwiye

<u>Article 8</u>: Appropriate Security Controls

<u>Article 8</u>: Contrôles appropriés de sécurité

Uwahawe uruhushya agomba gukora ku buryo igenzura ry'umutekano rikwiye rigaragazwa neza kandi rikorwa mu muyoboro we kugira ngo yirinde ibyawuhungabanya byaba ibizwi cyangwa ibitazwi. Imicungire y'umutekano w'amakuru (ISMS) igomba gushyirwa mu bikorwa hakubiyemo ibintu by'ingenzi bikurikira:

(a) Isuzuma ry'ibibazo bishobora kuvuka;
(b) Politiki z'umutekano w'amakuru;
(c) Imicungire y'umutungo;

The Licensee shall ensure that appropriate security controls are clearly documented and set in their network and systems against various known and unknown threats. A comprehensive Information Security Management System (ISMS) must be implemented including the essential components hereunder:

(a) Risk Assessment;
(b) Information security policies
(c) Asset management

Le titulaire de licence doit s'assurer que les contrôles de sécurité appropriés sont clairement documentés et mis en place dans son réseau et ses systèmes contre diverses menaces connues et inconnues. Un système de gestion de sécurité de l'information (ISMS) doit être mis en œuvre, y compris les éléments essentiels ci-dessous :

(a) Evaluation des risques;
(b) Politiques de sécurité de l'information
(c) Gestion des biens

(d) Kugenzura uburyo bwo kugera ku makuru;
(e) Imicungire y'itumanaho n'ibikorwa;

(f) Imicungire y'itunganya;
(g) Imicungire y'impinduka;
(h) Imicungire y'ibibazo bishobora kuvuka;
(i) Kubona, gukora no kubungabunga porogaramu y'ikoranabuhanga;
(j) Gahunda y'ikomeza ry'ibikorwa by'ubucuruzi na gahunda yo gusubukura imirimo nyuma y'ibiza;
(k) Gusuzuma ahashobora kwibasirwa no kugenzura
(l) Igerageza ryo kwinjira kw'abagenzuzi b'imbere cyangwa bo hanze bemewe n'Urwego Ngenzuramikorere;
(m) Kugaragaza, kubungabunga no gukurikirana iyubahirizwa ry'amategeko n'amabwiriza;
(n) Imicungire y'uburyo kode zigenda zihererekanywa;
(o) Umutekano w'abakozi;
(p) Imicungire yo kugarura ibyatakaye.

(d) Access control
(e) Communications and operations management
(f) Configuration Management;
(g) Change Management;
(h) Incident Management;
(i) Secured application acquisition, development and maintenance;
(j) Business continuity plan and Disaster recovery plan;

(k) Vulnerability assessment and Audit;

(l) Internal and external penetration testing by auditors approved by the Regulatory Authority;
(m) Legal and Regulatory compliance identifying, maintaining and monitoring;
(n) Cryptographic algorithm management;
(o) Human resources security;
(p) Backup management.

(d) Contrôles d'accès
(e) Gestion des communications et des opérations
(f) Gestion de la configuration;
(g) Gestion du changement;
(h) Gestion des incidents;
(i) Acquisition, développement et maintenance sécurisés des applications;
(j) Planification pour la continuité des activités et pour la reprise après sinistre;

(k) Evaluation de la vulnérabilité et audit;

(l) Test de pénétration interne et externe par les auditeurs approuvés par l'Autorité de Régulation ;
(m) Identification, maintenance et suivi de la conformité aux lois et règlement ;

(n) Gestion d'algorithmes cryptographiques;

(o) Sécurité des ressources humaines ;
(p) Gestion des sauvegardes.

<u>Ingingo ya 9</u>: Gushyira ibice mu bikoresho by'imiyoboro

Umuyoboro wose ugomba kugira nibura ibice bitatu (3) bikurikira:
(a) Igice cy'imicungire;
(b) Igice cy'igenzura cyangwa amasezerano y'itumanaho;

<u>Article 9:</u> Establishment of Layers in Network Facilities

Any network facility must have at least three (3) layers which are as follows:
(a) Management plane;
(b) Signalling/Control plane or Communication protocol;

<u>Article 9</u>: Etablissement des couches dans les installations des réseaux

Toute installation de réseau doit avoir au moins trois (3) couches qui sont les suivantes:
(a) Couche de gestion ;
(b) Couche de signalisation/commande ou protocole de communication ;

(c) Igice cy'amakuru.

<u>Ingingo ya 10</u>: Akamaro k'ibice mu miyoboro

Igice gishinzwe imicungire gifite inshingano yo kurinda imicungire y'amakuru anyuzwa ku muyoboro n'imikorere y'umuyoboro, naho igice gishinzwe igenzura kigakoreshwa mu guha ibimenyetso amakuru no kuyaha icyerekezo. Igice gishinzwe amakuru gifite inshingano yo kohereza serivisi z'amakuru ku bikoresho koranabuhanga by'abafatabuguzi.

<u>Ingingo ya 11</u>: Kurinda igice cy'imicungire

Mu rwego rwo kurinda igice gishinzwe imicungire, abahawe impushya bose bagomba:

(a) Kugira no gukurikiza politiki na gahunda z'umutekano w'amakuru mu rwego rw'itumanaho;
(b) Gukora ku buryo muri buri gikorwa habaho itandukana ry'inshingano;
(c) Gukora ku buryo habaho itandukana ry'imiyoboro n'urusobe koranabuhanga;
(d) Gukumira ibishobora kugera mu muyoboro bitemewe kandi bitagenzuwe (harimo na porogaramu bijyanye);
(e) Kurinda amakuru bwite y'umufatabuguzi harimo n'ayerekeranye n'ububiko

(c) Data plane.

<u>Article 10</u>: Importance of Layers in the Network facilities

The management plane has the role of securing the network traffic management and network operation while the signalling plane is used for signalling and routing the traffic. The data plane has the role of delivering data services to the customer devices.

<u>Article 11</u>: Protection of the Management Plane

To protect the management plane, all licensees must:

(a) have and follow well defined industry information security policies and procedures;
(b) ensure segregation of duties in every process;
(c) ensure the segregation of Networks and systems;
(d) prevent unauthorized and uncontrolled access to network and systems (including related applications);
(e) secure the subscriber information such as personal information including but not

(c) Couches des données.

<u>Article 10</u>: Importance des couches dans les installations des réseaux

La couche de gestion a pour rôle de sécuriser la gestion du trafic réseau et le fonctionnement du réseau tandis que la couche de signalisation est utilisée pour la signalisation et le routage du trafic. La couche des données a pour rôle de fournir des services des données aux appareils des clients.

<u>Article 11:</u> Protection de la couche de gestion

Pour protéger la couche de gestion, tous les titulaires de licence doivent :

(a) avoir et suivre les politiques et les procédures bien définies de la sécurité de l'information de l'industrie;
(b) assurer la répartition des tâches dans chaque processus;
(c) assurer la séparation des réseaux et des systèmes;
(d) empêcher tout accès non autorisé et non contrôlé au réseau et aux systèmes (y compris les applications connexes);
(e) sécuriser les informations du souscripteur telles que les informations personnelles, y

bw'amajwi iyo buhari, inyemezabuguzi hamwe n'andi makuru ya ngombwa;

limited to Call Data Records (CDRs) where applicable, billing and other relevant information;

compris, mais sans se limiter, aux enregistrements des données d'appel (CDR) le cas échéant, la facturation et autre information importante ;

(f) Kugira uburyo buhoraho bwo kugarura amakuru;

(f) ensure a regular backup;

(f) assurer la récupération régulière ;

(g) Gusobanurira abakozi, abafatabuguzi n'abatanga serivisi, imicungire y'uburyo bwo kugera ku makuru no gukora ku buryo hatabaho ihakana ry'amakuru hashyirwaho uburyo buhamye bwo gusuzuma umwimerere wayo;

(g) define access control management for employees, subscribers and vendors based on the least privilege guidance and ensure the non-repudiation by implementing strong authentication controls;

(g) définir la gestion de contrôle d'accès pour les employés, les abonnés et les fournisseurs sur la base des conseils les moins privilégiés et garantir la non-répudiation en mettant en œuvre des contrôles forts d'authentification;

(h) Gukora isuzuma rihoraho ry'uburyo bwo kugera ku bikoresho no kuri porogaramu

(h) conduct a regular log review of devices access and application access;

(h) effectuer un examen régulier du journal d'accès aux appareils et d'accès aux applications;

(i) Gukora ku buryo habaho umutekano w'ikoranabuhanga hitabwa ku mitunganyirize yaryo no ku isuzuma ry'umutekano waryo;

(i) ensure the application security by secure development and performing security testing;

(i) assurer la sécurité de l'application par un développement sécurisé et effectuer des tests de sécurité;

(j) Kugira no gukurikiza nzira zikurikizwa mu kumenya umwirondoro w'umukiriya(« Know Your Customer (KYC) »

(j) have and follow well defined Know Your Customer (KYC) procedures;

(j) avoir et suivre les procédures bien définies « Know Your Customer (KYC) » ;

(k) Gukora ku buryo habaho umutekano w'uduce twose tw'amakuru, ibikoresho, urusobe koranabuhanga na porogaramu;

(k) ensure security hardening of all nodes, devices, systems and applications;

(k) assurer le renforcement de la sécurité de tous les nœuds, appareils, systèmes et applications;

(l) Kwemera gusa urusobe koranabuhanga, porogaramu na serivisi byasuzumwe kandi byizewe;

(l) only allow deployment and/or integration of tested and secured systems, applications and services;

(l) autoriser uniquement le déploiement et/ou l'intégration des systèmes, applications et services testés et sécurisés;

(m) Gukora ku buryo ingamba z'umutekano w'imbere zivugururwa kandi zikemezwa n'Urwego Ngenzuramikorere;

(m) Ensure that internal security policies are regularly updated and approved by the regulatory Authority;

(m) assurer que les politiques de sécurité internes soient régulièrement mises à jour et approuvées par l'Autorité de Régulation;

(n) Gukora ubugenzuzi buhoraho ku rusobe koranabuhanga, porogaramu na serivisi;
(o) Gusangiza abafatabuguzi amakuru igihe cyose havutse ikibazo
(p) kuburira abakozi buri gihe hakurikijwe ibyo bakora n'inshingano zabo no gukora ku buryo hajyaho uburyo bw'isuzumamikorere ry'abakozi biturutse kuri iryo burira;

(q) Kumenyesha abafatabuguzi, ikibazo cy'umutekano muri serivse zitangwa, ingamba yafata ngo yirinde icyo kibazo n'ikiguzi izo ngamba zishobora gutwara umufatabuguzi igihe arimo afata izo ngamba. Amakuru atanzwe kubera iyi mpamvu agomba guhabwa umufatabuguzi nta kindi kiguzi atanze uretse ikiguzi umufatabuguzi yaba yakoresheje kugira ngo agere kuri ayo makuru.

(r) Gushyiraho ingamba na gahunda binoze byo kuzahura urusobe koranabuhanga, muri porogaramu no muri serivisi;

(s) Kubika, kugaragaza, kugenzura no gusuzuma ibitabo bikubiyemo uburyo bwo kugera ku muyoboro wose, urusobe koranabuhanga na porogaramu;

(n) conduct regular audit on all systems, applications and services;
(o) Share information to subscribers whenever an incident occur ;
(p) occurs and regularly provide awareness to its employees depending on their roles and responsibilities and ensure means of evaluation of the performance of employees as a result of such awareness;

(q) inform subscribers of the risks to the security of provided services, appropriate measures that the subscriber may take to safeguard against the risks and the likely costs to the subscriber involved in the taking of such measures. Information provided for this purpose must be provided to the subscriber free of any charge other than the cost that the subscriber would have incurred for accessing the information.

(r) provide adequate contingency plans and arrangements in their systems, applications and services;

(s) maintain, document, control and monitor all access logs of all network, systems and applications;

(n) effectuer un audit régulier de tous les systèmes, applications et services;
(o) Partager les informations aux abonnés chaque fois qu'un incident se produit
(p) informer régulièrement ses employés en fonction de leurs rôles et responsabilités et assurer des moyens d'évaluation de la performance des employés à la suite de cette sensibilisation ;

(q) informer les abonnés des risques pour la sécurité des services fournis, des mesures appropriées que l'abonné peut prendre pour se prémunir contre les risques et des coûts probables pour l'abonné impliqué dans la prise de telles mesures. Les informations fournies à cet effet doivent être fournies à l'abonné sans aucun frais autre que le coût que l'abonné aurait encouru pour accéder à l'information.

(r) fournir des plans d'intervention et des dispositions adéquats dans leurs systèmes, applications et services;

(s) conserver, documenter, contrôler et surveiller tous les registres d'accès de tous les réseaux, systèmes et applications;

(t) Kugaragaza, kugenzura no gusuzuma uburyo bwose bwa kure bwo kugera ku duce tw'amakuru no ku rusobe koranabuhanga mu rwego rwo gutunganya, gukosora, kubika, kwinjira, gutanga, gukora inyemezabuguzi no kwita ku mufatabuguzi;

(u) Gushyira mu bikorwa igenzura mu rwego rwo gukumira ko hari uwagera ku muyoboro we mu buryo butemewe.

(t) document, control and monitor all remote access to nodes and systems for configuring, patching, backup, logging, provisioning, billing and subscriber care;

(u) Implement controls to prevent fraudulent access to their network and systems.

(t) documenter, contrôler et surveiller tous les accès à distance aux nœuds et aux systèmes pour la configuration, l'application de correctifs, la récupération, l'accès, l'approvisionnement, la facturation et les soins aux abonnés;

(u) Mettre en œuvre des contrôles pour empêcher l'accès frauduleux à leur réseau et à leurs systèmes.

Hashingiwe kuri iyi ngingo, uwahawe uruhushya agomba gukora ku buryo ahora agarura ibikozwe byose ku muyoboro no ku rusobe koranabuhanga kandi, igihe cyose hari impinduka zikozwe, ibyo byabitswe bikaba bigomba kuba bimeze nk'uko byari biri bitarahinduka.

Under this provision, the licensee shall ensure regular network and system configuration backups and, whenever any change is incorporated, the backed-up configurations must be identical to the running configurations prior to the change.

En vertu de cette disposition, le titulaire de licence doit assurer des récupérations régulières de la configuration du réseau et du système et, chaque fois qu'un changement est incorporé, les configurations sauvegardées doivent être identiques aux configurations en cours d'exécution avant le changement.

Andi makuru ajyanye n'umufatabuguzi nk'ibitabo, amakuru agarurwa ajyanye n'umuyoboro bigomba kugira gahunda ya buri munsi, buri kwezi na buri mwaka.

Other customer related information such as Logs, business and network information backups must have daily, monthly and annual plans.

Les autres informations relatives au client telles que les registres, les récupérations d'informations commerciales et de réseau doivent avoir des plans quotidiens, mensuels et annuels

<u>Ingingo ya 12</u>: Kurinda igice cy'igenzura

<u>Article 12</u>: Protection of the Signalling or Control Plane

<u>Article 12</u> : Protection du plan de signalisation ou de commande

Uwahawe uruhushya agomba buri gihe kurinda abafatabuguzi be ibi bikurikira:

The licensee must always ensure protection of their subscribers against:

Le titulaire de licence doit toujours assurer la protection de ses abonnés contre:

(a) Igenzura ry'amakuru ritagaragara n'irigaragara;

(b) Kwiyitirira undi muntu;

(a) Passive and active interception;

(b) Impersonation;

(a) l'interception passive et active;

(b) l'usurpation d'identité;

(c) Gukurikirana umufatabuguzi no kubasha kubona ibimenyetso byasizwe n'uwakoresheje ikoranabuhanga.

Mu gukaza umutekano w'abafatabuguzi, uwahawe uruhushya agomba:

i) Gusuzuma no kwemeza abafatanyabikorwa bose;
ii) Kwemeza ibyo abafatanyabikorwa bashyizemo;
iii) Gutuma ahatangirwa ibimenyetso hatagenzurwa n'igice cy'amakuru cyangwa ngo hagerweho bitanyuze mu gice cy'igenzura;
iv) Gukora igenzura ryo kwemeza ibikoresho biri ku miyoboro y'utanga serivisi hagamijwe kureba ko nta bikoresho bitemewe bishobora gushyirwaho;
v) Gukora ku buryo amakuru yose yinjira n'asohoka yemezwa kandi akayungururwa;
vi) Kugira akarindabutumwa gashinzwe kugenzura no gukurikirana ihererekanya ry'ubutumwa bugufiaho bishoboka;
vii) Gukora ku buryo habaho umutekano ukomeye w'ibikoresho na porogaramu koranabuhanga.

<u>Ingingo ya 13</u>: Kurinda igice cy'amakuru

Uwahawe uruhushya agomba kurinda igice kirimo amakuru mu rwego rwo kwirinda

(c) Subscriber tracking and traceability of digital footprints.

To enhance the security of the subscribers, the licensee must:

i) Verify and validate all signalling partners;
ii) Validate all external input originating from signalling partners;
iii) Prevent signalling points from being addressable from the either the data plane or being accessible from outside of the Control plane;
iv) Implement controls to validate the end devices on operator's networks to ensure that no unauthorized devices are able to connect;
v) Ensure that all the incoming and outgoing traffic are validated and filtered;
vi) Have SMS firewall to control and monitoring SMS traffic where applicable;
vii) Ensure security hardening the devices and applications.

<u>Article 13</u>: Protection of the data plane

The licensee shall protect the data plane to avoid cyber-attack and data breaches and

(c) le suivi des abonnés et la traçabilité des empreintes numériques.

Pour renforcer la sécurité des abonnés, le titulaire de licence doit :

i) vérifier et valider tous les partenaires de signalisation;
ii) valider toutes les entrées externes provenant des partenaires de signalisation;
iii) empêcher les points de signalisation d'être adressables depuis le plan des données ou accessibles depuis l'extérieur de la couche de commande;
iv) mettre en œuvre les contrôles pour valider les appareils terminaux sur les réseaux des opérateurs afin de garantir qu'aucun appareil non autorisé ne peut se connecter;
v) s'assurer que tout le trafic entrant et sortant est validé et filtré;
vi) disposer d'un pare-feu SMS pour contrôler et surveiller le trafic SMS le cas échéant ;
vii) Assurer la sécurité forte des appareils et des applications.

<u>Article 13 :</u> Protection de la couche des données

Le titulaire de licence doit protéger la couche des données pour éviter les cyberattaques et les

ibitero by'ikoranabuhanga n'ibyahungabanya amakuru no kugabanya ibyago byagwirira umuyoboro , urusobe koranabuhanga na serivise.

<u>Ingingo ya 14:</u> Iby'ingenzi bisabwa mu igenzura ry'igice cy'amakuru

Uwahawe uruhushya agomba gukora iby'ingenzi bikurikira mu igenzura ry'amakuru:

(a) Kuyungurura no gukurikirana ihererekanya ry'amakuru;
(b) Kurinda ibanga n'ubusugire bw'amakuru;
(c) Gukurikirana no gusuzuma ihererekanya ry'amakuru harimo n'aho yaturutse;
(d) Gushyiraho uburyo bwo gutahura no gukumira mu rwego rwo kwirinda ibyahungabanya umuyoboro n'ibyawinjiramo mu buryo butemewe;
(e) Gushyiraho ibibujijwe aho bibaye ngombwa;
(f) Gukora ku buryo hajyaho ubushobozi bwo kugaragaza no gukurikirana inenge iyo ari yo yose;
(g) Amakuru yose yerekeye umufatabuguzi yoherejwe cyangwa yagezweho binyuze mu muyoboro uwo ari wo wose cyangwa VPN agomba kurindwa hakoreshejwe code z'ibanga zemewe mu ikoranabuhanga mu rwego rwo kurinda umwimerere n'ibanga by'amakuru.

mitigate the risk on their network, systems and services.

<u>Article 14:</u> Required Minimum Controls for Data Plane

The Licensee shall put in place the following minimum controls which include but are not limited to:

(a) filter and monitor of traffic data;
(b) ensure data confidentiality, integrity and availability;
(c) monitor and verify all traffic including their originating source;
(d) ensure implementation of intrusion, detection, and prevention systems to protect against network intrusions and unauthorised access;
(e) use traffic restriction where deemed necessary;
(f) ensure capacity to identify and monitor any abnormalities;
(g) subscriber's information transferred or accessed through any channel or VPN links shall be protected with industry recommended encryption standards to ensure the authenticity and confidentiality of data.

violations des données et atténuer les risques sur son réseau, ses systèmes et service.

<u>Article 14:</u> Contrôles minimaux requis pour la couche des données

Le titulaire de licence doit mettre en place les contrôles minimaux suivants sans toutefois s'y limiter :

(a) filtrer et surveiller les données de trafic;
(b) assurer la confidentialité, l'intégrité et la disponibilité des données;
(c) surveiller et vérifier tout le trafic, y compris son origine;
(d) assurer la mise en œuvre des systèmes d'intrusion, de détection et de prévention pour se protéger contre des intrusions sur le réseau et des accès non autorisés;
(e) utiliser les restrictions du trafic lorsque cela est jugé nécessaire;
(f) assurer la capacité d'identifier et de surveiller toute anomalie;
(g) les informations de l'abonné transférées ou accessibles via n'importe quel canal ou lien VPN doivent être protégées par des normes de cryptage recommandées par l'industrie pour garantir l'authenticité et la confidentialité des données.

(h) Gukoresha urufunguzo rw' ikoranabuhanga(PKI) mu rwego rwo kurinda umutekano w'ihererekanya ry'amakuru koranabuhanga, aho bishoboka.

(h) use of digital certificates (PKI) to ensure secure electronic transactions where applicable.

(h) utiliser des certificats numériques (PKI) pour garantir des transactions électroniques sécurisées, le cas échéant.

Ingingo ya 15: Imicungire n'irindwa ry'imiyoboro n'urusobe koranabuhanga

Imiyoboro yose, urusobe koranabuhanga na porogaramu koranabuhanga by'uwahawe uruhushya ntibigomba gucungwa, gucumbikira, kwinjirwamo cyangwa gushyirwa hanze ya Repubulika y'u Rwanda keretse bibanje gutangirwa uburenganzira bweruye n'Urwego Ngenzuramikorere.

Article 15: Management and Protection of Networks and Systems

All networks, systems and applications of the licensee shall not be managed, hosted, remotely accessed or located outside of the Republic of Rwanda unless explicitly authorized by the Regulatory Authority.

Article 15: Gestion et protection des réseaux et des systèmes

Tous les réseaux, systèmes et applications du titulaire de licence ne doivent pas être gérés, hébergés, accessibles à distance ou situés en dehors de la République du Rwanda, sans autorisation expresse de l'Autorité de Régulation.

Ingingo ya 16: Amakuru yerekeye nomero ya telefoni ihamagaye

Telefoni zose zihamagariye mu Rwanda zihamagara imbere mu Rwanda zigomba kugaragaza nomero ihamagaye. Uburyo bwose buyihisha ntibwemewe keretse ubwemejwe n'Urwego Ngenzuramikorere.

Umufatabuguzi wifuza ko nimero ye itagaragara abisabira uburenganzira Urwego Ngenzuramikorere, yabuhabwa akabuha uwahawe uruhushya kugira ngo abishyire mu bikorwa.

Article 16: Call ID Information

All local incoming calls originating from within Rwanda shall have Caller Identification. Any masking feature shall not be allowed except for those approved by the Regulatory Authority.

Any subscriber who wishes to have the masking feature applied to his/her number must seek authorisation from the Regulatory Authority and if granted, submit the authorisation to the Licensee for implementation.

Article 16 : Information d'identification de l'appel

Tous les appels locaux entrants en provenance du Rwanda doivent avoir l'identification de l'appelant. Aucune fonction de masquage n'est autorisée, à l'exception de celles approuvées par l'Autorité de Régulation.

Tout abonné souhaitant que la fonction de masquage soit appliquée à son numéro doit obtenir l'autorisation de l'Autorité de Régulation et, si elle est accordée, soumettre l'autorisation au titulaire de licence pour sa mise en œuvre.

Ingingo ya 17: Kwegurira undi muntu urusobe n'ibikorwa koranabuhanga

Mbere yo kwegurira undi muntu urusobe koranabuhanga, ibikorwa na serivisi koranabuhanga, uwahawe uruhushya abisabira uburenganzira Urwego Ngenzuramikorere kandi agomba kuba azi ko uwo muntu yahawe uruhushya n'Urwego Ngenzuramikorere mbere yo gukora andi masezerano.

Undi muntu uwo ari we wese ushaka gukora ibikorwa bijyanye na ICT ku isoko ry'u Rwanda, agomba kwemererwa n'Urwego Ngenzuramikorere.

Uwahawe uruhushya wese wifuza kwegurira cyangwa weguriye undi muntu ibikorwa bye agomba no kumuha gahunda y'ibijyanye n'umutekano wabyo.

Uwahawe uruhushya agomba kugira umuyobozi mukuru ushinzwe tekiniki, ushinzwe ikoranabuhanga cyangwa indi mirimo nka yo, b'abanyarwanda bashinzwe ibikorwa remezo by'umuyoboro n'iby'ikoranabuhanga, igenamigambi n'ibikorwa.

Article 17: Outsourcing Systems and Operations to a Third Party

Before outsourcing any of its systems, operations or services to any third party, the Licensee shall seek approval from the Regulatory Authority and ensure that all third parties are licensed by the Regulatory Authority prior to any contractual engagement.

Any third party who wants to operate on the Rwanda ICT market shall be approved by the Regulatory Authority.

Any Licensee willing or having outsourced their systems and operations to any third party must extend their security framework to the third party.

The Licensee is required to have a Rwandan as its Chief Technical Officer (CTO), Chief Information officer (CIO) or equivalent functions, responsible for its network technical and Information technology infrastructure, systems planning and operations.

Article 17: Externalisation des systèmes et des opérations à un tiers

Avant d'externaliser l'un de ses systèmes, opérations ou services à un tiers, le titulaire de licence doit demander l'approbation de l'Autorité de Régulation et s'assurer que tous les tiers sont autorisés par l'Autorité de Régulation avant tout engagement contractuel.

Tout tiers souhaitant opérer sur le marché rwandais des TIC doit être autorisée par l'Autorité de Régulation.

Tout titulaire de licence souhaitant ou ayant externalisé ses systèmes et opérations à un tiers doit étendre son cadre de sécurité au tiers.

Le titulaire de licence doit avoir un Rwandais dans les fonctions de chef de direction technique, chef du service de l'information ou fonctions équivalentes, chargé de son infrastructure technique et informatique de réseau, de la planification des systèmes et des opérations.

Ingingo ya 18: Ibisabwa mu kwegurira undi muntu urusobe n'ibikorwa koranabuhanga

Nyuma yo kwemererwa kwegurira undi muntu urusobe n'ibikorwa koranabuhanga, uwahawe uruhushya agomba:

(a) gusobanura ibijyanye n'umutekano mu guhitamo undi muntu;
(b) gutegura amasezerano n'undi muntu arimo ibijyanye n'umutekano w'amakuru na KPI cyangwa amasezerano agena imitangire ya serivisi;
(c) gushyira mu bikorwa ibyavuye mu isuzuma ry'ibibazo bishobora kuvuka hamwe n'undi muntu;
(d) gukora isuzuma ry'abandi bantu bose, imiryango n'ubumenyi bw'abakozi bafite uruhare mu bikorwa no mu micungire y'urusobe koranabuhanga;
(e) guhuza politiki y'umutekano y'undi muntu n'ibisabwa n'uwahawe uruhushya bijyanye n'umutekano;
(f) gukora isuzuma rihoraho n'igenzura ku bandi bantu;
(g) kugeza ku bandi bantu gahunda y'ikomeza ry'ibikorwa by'ubucuruzi irenga imipaka y'ikagera ku wundi muntu.

Article 18: Conditions of Outsourcing the System and Operations to a Third Party

After the approval to outsource the system and operation to any third party, the licensee is required to:

(a) define detailed security process for selection of third party;
(b) design contracts with third parties containing information security requirements and KPIs or SLAs;
(c) implement a structured risk assessment process with third parties;
(d) perform background verification of all the third parties, Organisations and employees' technical skill sets involved in the operations and management of the systems;
(e) align the security policy of the third parties with the Licensee's security requirements;
(f) conducting regular review and audit on the third parties;
(g) extend the business continuity beyond organizational boundaries to third parties.

Article 18: Conditions d'externalisation du système et des opérations à un tiers

Après l'approbation d'externaliser le système et les opérations à un tiers, le titulaire de licence est tenu de:

(a) définir le processus de sécurité détaillé pour la sélection d'un tiers;
(b) concevoir des contrats avec des tiers contenant des exigences de sécurité de l'information et des KPI ou SLA;
(c) mettre en œuvre un processus structuré d'évaluation des risques avec des tiers ;
(d) effectuer une vérification des antécédents de tous les ensembles de compétences techniques des tiers, des organisations et des employés impliqués dans les opérations et la gestion des systèmes ;
(e) aligner la politique de sécurité des tiers sur les conditions de sécurité du titulaire de licence ;
(f) mener des examens et des audits réguliers sur les tiers ;
(g) étendre la continuité des activités au-delà des frontières organisationnelles aux tiers.

<u>Ingingo ya 19</u>: Inzira zikurikizwa mu gusaba uburenganzira

Uwahawe uruhushya usaba uburenganzira buvugwa muri aya mabwiriza yandikira Urwego Ngenzuramikorere arusaba uburenganzira cyangwa icyemezo cy'uko rwabyemeye.

Uwahawe uruhushya asobanura impamvu z'ubusabe bwe kandi agatanga amakuru ahagije kugira ngo Urwego Ngenzuramikorere rubashe gufata icyemezo gikwiye mu gihe gikwiye.

Uburenganzira buhabwa ubusaba nyuma yo kwakira ubusabe na nyuma yo kuzuza ibisabwa n'Urwego Ngenzuramikorere. Nyuma y'isesengura, Urwego Ngenzuramikorere rushobora gutanga cyangwa kudatanga uburenganzira bwasabwe kandi iyo ibisabwa bitubahirijwe, usaba amenyeshwa mu nyandiko icyemezo cy'Urwego Ngenzuramikorere.

<u>Article 19</u>: Authorization Procedures

The licensee requesting for authorization specified in this regulation shall write to the Regulatory Authority requesting an authorization or non-objection to do so.

The licensee shall justify the reason for the approval and must provide sufficient information to allow the Regulatory Authority take appropriate decision in a timely manner.

Approvals shall be granted to the licensee after receipt of the request and after fulfilment of the regulatory requirements. Upon the result of its assessment, the Regulatory Authority may or not grant the authorization requested and in the event of failure to comply with the requirements for approval, the licensee shall be notified in writing of the Regulatory Authority's decision.

<u>Article 19</u> : Procédures d'autorisation

Le titulaire de licence qui demande l'autorisation spécifiée dans le présent règlement doit s'adresser par écrit à l'Autorité de Régulation pour demander une autorisation ou une non-objection à cet effet.

Le titulaire de licence doit justifier le motif de la demande et doit fournir des informations suffisantes pour permettre à l'Autorité de Régulation de prendre une décision appropriée en temps opportun.

Les approbations sont accordées au titulaire de licence après réception de la demande et après satisfaction aux conditions réglementaires. A l'issue de son évaluation, l'Autorité de Régulation peut ou non accorder l'autorisation demandée et en cas de non-respect des conditions d'approbation, le titulaire de licence est informé par écrit de la décision de l'Autorité de Régulation.

UMUTWE WA IV: ISUZUMA RY'UMUTEKANO N'UBUGENZUZI BW'IMIYOBORO N'URUSOBE KORANABUHANGA BY'UWAHAWE URUHUSHYA

Ingingo ya 20: Isuzuma ry'umutekano w'ibice byose

Uwahawe uruhushya akora buri mwaka isuzuma ryo kureba intege nke n'iryo kwinjira mu bice by'umuyoboro kugira ngo arebe ahari intege nke bityo azikemure mu buryo bwihuse.

Iryo suzuma rikorwa n'umuntu wo hanze kandi wigenga kandi raporo yaryo igahabwa Urwego Ngenzuramikorere ikimara gukorwa.

Ingingo ya 21: Isuzuma ryo kureba ahashobora kwibasirwa.

Iyo bakora isuzuma ryo kureba ahasobora kwibasirwa ku miyoboro yabo, abahawe impushya bagomba:

(a) kugira ibikoresho bisuzuma na porogaramu bifite uburyo bukoreshwa n'umuntu cyangwa bwikoresha;
(b) gukora isuzuma ryo kureba ahashobora kwibasirwa ku bice byose;

CHAPTER IV: SECURITY ASSESSEMENT AND AUDIT OF NETWORKS AND SYSTEMS OF LICENSEES

Article 20: Security Assessment of All Planes

The licensee shall perform a vulnerability assessment and penetration testing for all planes to identify the weaknesses and fix them in a timely manner on annual basis.

Such assessment shall be conducted by an external and independent party and the report must be shared with the Regulatory Authority as soon as it is available.

Article 21: Vulnerability Assessment

To conduct the vulnerability assessment of their network and systems, the licensees must:

(a) have test devices, nodes and applications with manual or automated tools;
(b) conduct vulnerability assessment on all the planes.

CHAPITRE IV: EVALUATION DE LA SECURITE ET AUDIT DES RESEAUX ET DES SYSTEMES DES TITULAIRES DE LICENCE

Article 20 : Evaluation de la sécurité de toutes les couches

Le titulaire de licence doit effectuer une évaluation de vulnérabilité et des tests de pénétration pour tous les plans afin d'identifier les faiblesses et de les corriger en temps opportun sur une base annuelle.
Cette évaluation doit être effectuée par un tiers externe et indépendant et le rapport doit être communiqué à l'Autorité de Régulation dès qu'il est disponible.

Article 21 : Evaluation de la vulnérabilité

Pour effectuer l'évaluation de la vulnérabilité de leur réseau et de leurs systèmes, les titulaires de licence doivent :

(a) disposer des appareils des tests, des nœuds et d'applications avec des outils manuels ou automatiques ;
(b) effectuer une évaluation de la vulnérabilité de tous les couches ;

(c) gukora isuzuma ry'umutekano mbere y'uko imiyoboro ihabwa uburenganzira bwo gutangira gukora;
(d) gukemura icyo kibazo cy'ahashobora kwibasirwa hashyirwaho utuntu dukosora hakanakorwa igenamiterere ryizewe;
(e) gukora ku buryo ibice byose bigira umutekano hakorwa isuzuma rihoraho ry'ibibazo bishobora kuvuka kuri buri gice mu rwego rwo kubikemura.

<u>Ingingo ya 22:</u> Ubugenzuzi bw'imbere

Buri mwaka, abahawe impushya bagomba gukora ubugenzuzi bwigenga, bugamije bureba niba imiyoboro ifite umutekano kandi yubahiriza amabwiriza mu rwego rwo gusuzuma icyo amasuzuma y'umutekano yagezeho ni ukuvuga igenzura ry'imicungire, igenzura mu bya tekiniki n'iryo mu bikoresho. Ubwo bugenzuzi bugomba kandi guhita bukorwa nyuma yo kugaragara kw'ikibazo gikomeye cyangwa nyuma yo kuvugurura urusobe koranabuhanga.

Uwahawe uruhushya agomba gupima icyo amagenzura yakozwe yagezeho kandi kuri buri nenge cyangwa kunanirwa uwahawe uruhushya agomba guhita akora uko yateganije ngo bikemuke.

Bitewe n'imiterere y'ibyavuye mu isuzuma, imirimo yo gukemura ibibazo ishobora kugeza

(c) perform security testing prior to systems being granted approval to move into production;
(d) fix the identified vulnerabilities by applying patches or secure configuration;
(e) ensure that all planes are secure by conducting regular risk assessments on each plane to identify and respond to unacceptable risks.

<u>Article 22:</u> Internal Audit

The Licensees shall on annual basis, conduct an independent security and compliance audit to verify the effectiveness of the implemented security controls such as management, technical and physical controls. Such audit must also be conducted immediately after a critical/major incident or following a system upgrade.

The Licensee shall measure the effectiveness of implemented controls and on any controls' shortfall or failure, the licensee must implement the remediation plan as soon as possible.

Depending in the nature of the audit findings, the remediation plan may be extended but not

(c) effectuer des tests de sécurité avant que les systèmes ne soient autorisés à passer par la production ;
(d) corriger les vulnérabilités identifiées en appliquant des correctifs ou une configuration sécurisée ;
(e) s'assurer que tous les couches sont sécurisées en effectuant des évaluations régulières des risques sur chaque plan pour identifier et traiter les risques inacceptables.

<u>Article 22:</u> Audit interne

Les titulaires de licence doivent, annuellement, mener un audit indépendant de sécurité et de conformité pour vérifier l'efficacité des contrôles de sécurité en cours tels que les contrôles de gestion les contrôles techniques et les contrôles physiques. Cet audit doit également être effectué immédiatement après un incident critique/majeur ou après une mise à niveau du système.

Le titulaire de licence doit mesurer l'efficacité des contrôles en cours et sur chaque défaillance ou échec de tout contrôle, le titulaire de licence doit effectuer le plan de remédiation le plutôt possible.

Selon la nature des constatations de l'audit, le plan de remédiation peut être prolongé mais ne

ariko ntirenze amezi atatu(3) bitewe n'uko byagenwa n'Urwego Ngenzuramikorere.

Ingingo ya 23: Igenzura nzibacyuho

Mu gihe hakenewe gufatwa icyemezo cy'imicungire cyangwa gukosora inenge byaratinze, uwahawe uruhushya agomba kugaragaza igenzura nzibacyuho rikwiye hanyuma akabona kurishyira mu bikorwa.

Ingingo ya 24: Koroshya ibibazo byatuma abafatabuguzi babura serivisi

Uwahawe uruhushya agomba kuba gushyiraho politiki n'uburyo bwo kurinda umutekano no koroshya ibibazo byose bizwi bishingiye kuri serivisi zitangwa mu rwego rwo kwirinda ko urusobe koranabuhanga rwangirika cyangwa ntirukore, bishobora kurogoya serivisi z'umufatabuguzzi cyangwa bigatuma abafatabuguzi bagira ibihombo.

Ingingo ya 25: Itangwa rya raporo y'isuzuma ryúmutekano n'iy'ubugenzuzi

Uwahawe uruhushya agomba kugeza raporo z'isuzuma n'ubugenzuzi na raporo za gahunda y'ubugenzuzi, ku Rwego Ngenzuramikorere mu gihe kitarenze iminsi mirongo itatu (30) nyuma y'isuzuma n'igenzura.

exceed three (3) months as may be determined by the Regulatory Authority.

Article 23: Compensatory Controls

Where there is management decision required or delay in acquisition to correct controls deficiencies, the licensee shall identify appropriate compensatory controls and implement the same.

Article 24: Mitigation of risks leading to subscribers' loss of service

The licensee shall put in place must have documented security policies and procedures to mitigate all known risks associated with the services offered to avoid damage to, or failure of systems, which may cause interruptions of subscriber's services or make subscribers suffer from such losses.

Article 25: Submission of the Security Assessment and Audit Report

Any licensee must submit the assessment and audit reports, audit plan reports, to the Regulatory Authority not later than thirty (30) calendar days after completion of the assessment and audit.

doit pas dépasser trois (3) mois, selon de la détermination de l'Autorité de Régulation.

Article 23: Contrôles compensatoires

Lorsque la décision de gestion est requise ou le retard dans l'acquisition pour corriger les lacunes de contrôles, le titulaire de permis doit identifier les contrôles compensatoires appropriés et les mettre en œuvre.

Article 24: Atténuation des risques entraînant la perte des services des abonnés

Le titulaire de licence doit mettre en place des documents contenant des politiques et des procédures de sécurité pour atténuer tous les risques connus associés aux services fournis afin d'éviter des dommages ou des défaillances des systèmes, qui peuvent interrompre les services de l'abonné ou faire en sorte que les abonnés souffrent de telles pertes.

Article 25: Présentation de rapport d'évaluation de sécurité et d'audit

Tout titulaire de licence doit soumettre les rapports d'évaluation et d'audit, les rapports du plan d'audit, à l'Autorité de Régulation au plus tard trente (30) jours calendriers après la fin d'évaluation et d'audit.

Ingingo ya 26: Gahunda yo gukosora inenge

Uwahawe uruhushya agomba gushyikiriza Urwego Ngenzuramikorere gahunda yo gukosora inenge hamwe na raporo z'ubugenzuzi.

Article 26: Remediation Plan

The licensee shall submit the remediation plan to the Regulatory Authority along with the audit reports.

Article 26 : Plan de correction

Le titulaire de licence doit soumettre le plan de correction à l'Autorité de Régulation avec les rapports d'audit.

Ingingo ya 27: Ubugenzuzi bw'Urwego Ngenzuramikorere

Uwahawe uruhushya agomba gukurikiza aya mabwiriza kandi Urwego Ngenzuramikorere rukora ubugenzuzi buri mwaka cyangwa igihe cyose bibaye ngombwa. Inenge zose zagaragajwe ku muyoboro no mu rusobe koranabuhanga zigomba kumenyeshwa abahawe impushya kugira ngo bazikosore. Gahunda yo gukosora inenge ishyikirizwa Urwego Ngenzuramikorere mu gihe kitarenze iminsi mirongo itatu (30) nyuma ya raporo y'ubugenzuzi.

Article 27: Regulatory Authority Audit

The licensee shall comply with this regulation and the Regulatory Authority shall conduct audit on annual basis or at any time when need arises. All network and system vulnerabilities identified shall be communicated to licensees for remediation. A remediation plan shall be submitted to the regulatory Authority not later than thirty (30) days after the audit report.

Article 27 : Audit de l'Autorité de Régulation

Le Titulaire de License doit se conformer à ce règlement et l'Autorité de Régulation doit effectuer un audit annuel ou à tout moment que le besoin se présente. Toutes les vulnérabilités du réseau et du système identifié doivent être communiquées aux titulaires de licence pour la correction. Le plan de correction doit être soumis à l'Autorité de Régulation au plus tard trente (30) jours après le rapport d'audit.

Uwahawe uruhushya agomba korohereza abagenzuzi abagezaho amakuru n'ibimenyetso babasabye.

The licensee is required to facilitate the auditors by providing requested information and evidence.

Le titulaire de licence est tenu de faciliter les auditeurs en leur fournissant les informations et les preuves demandées.

Urwego Ngenzuramikorere rugomba kumenyesha uwahawe uruhushya y'ibyumweru bibiri (2) mbere y'uko ubugenzuzi bukorwa.

The Regulatory Authority shall issue notification to the licensee two (2) weeks prior to conducting the regulatory security audit.

L'Autorité de Régulation doit informer le titulaire de licence endéans deux (2) semaines avant de conduire l'audit de sécurité règlementaire.

UMUTWE WA V: IMICUNGIRE IHAMYE Y'IBIBAZO

Ingingo ya 28: Imicungire y'ibibazo

Uwahawe uruhushya agomba kurinda umuyoboro we n'urusobe koranabuhanga rwe, akora ariko atagarukira kuri ibi bikurikira:

(a) kumenyekanisha ikibazo cy'umutekano n'inzira zo kugikemura;

(b) uburyo bw'imicungire y'ikibazo n'amahugurwa y'abakozi ku ikoreshwa ry'izo nzira mu gihe habaye ikintu kibangamye;

(c) imirongo ngenderwaho mu kugaragaza ikibazo nk'ikibazo cy'umutekano;

(d) inzira z'itumanaho zikoreshwa mu kumenyekanisha ikibazo cy'umutekano;

(e) kwandika ibibazo by'umutekano byamenyekanishijwe;

(f) guha agaciro ibibazo by'umutekano;

(g) uburyo bwo kumenyekanisha ibibazo by'umutekano;

(h) gukemura no gupfundikira ibibazo;

(i) isesengurampamvu riganisha ku inoza ry'imikorere;

CHAPTER V: EFFECTIVE MANAGEMENT OF INCIDENTS

Article 28: Incident Management

The Licensee must protect their networks and systems, which include but is not limited to:

(a) implementation of a security incident reporting and handling process;

(b) incident Management process and training of its employees on how to use the processes in the event of any adverse event.

(c) guidelines for identifying any incident as a security incident;

(d) communication channels to be used for reporting the security incident;

(e) recording security incidents reported;

(f) assigning severity to security incidents;

(g) escalation mechanism for security incidents;

(h) resolution and closure of incidents;

(i) root cause analysis leading to process improvements;

CHAPITRE V : GESTION EFFICACE DES INCIDENTS

Article 28 : Gestion des incidents

Le titulaire de licence doit protéger ses réseaux et systèmes, y compris, mais sans se limiter :

(a) à la mise en œuvre d'un processus de signalement et de traitement des incidents de sécurité;

(b) au processus de gestion des incidents et la formation de ses employés sur la façon d'utiliser les processus en cas d'événement indésirable;

(c) aux lignes directrices pour identifier tout incident comme incident de sécurité;

(d) aux canaux de communication à utiliser pour signaler l'incident de sécurité;

(e) à l'enregistrement des incidents de sécurité signalés;

(f) qualifier la gravité des incidents de sécurité;

(g) aux mécanismes d'escalade pour les incidents de sécurité;

(h) à la résolution et la clôture des incidents;

(i) à l'analyse de causes profondes conduisant aux améliorations des processus;

(j) gukora raporo ya buri kwezi hagamijwe isesengurampamvu;
(k) gushyiraho itsinda ry'imbere rishinzwe imicungire y'ibibazo rigakorana n'itsinda rishinzwe gukemura ibibazo by'umutekano wa mudasobwa mu rwego rwo gukemura ibibazo by'umutekano mu buryo buhamye.

Uko ibibazo bivugwa muri iyi ngingo bishyirwa mu byiciro, biri ku ***Mugereka wa Mbere*** w'aya mabwiriza.

<u>Ingingo ya 29:</u> Guhanahana amakuru ajyanye n' ibibazo by'umutekano

Uwahawe uruhushya cyangwa buri wese utanga serivisi ukorana n'uwahawe uruhushya agomba guhita amenyesha Urwego Ngenzuramikorere ibibazo byose by'umutekano byavutse bifatwa nk'ibikomeye nk'uko bisobanurwa mu ***MUGEREKA WA MBERE*** w'aya Mabwiriza mu masaha 24 ikibazo kikivuka hakoreshejwe E-mail yatanzwe n'Urwego Ngenzuramikorere.

Imenyekanisha rya mbere ry'ibibazo byihutirwa rikorwa n'uwahawe uruhushya mu masaha 3 uhereye igihe ikibazo cyabereye hifashishijwe E-mail y'Urwego Ngenzuramikorere.

(j) monthly report to business for root cause analysis;
(k) creating an internal incident management team to work in cooperation with government CSIRT (Computer Security Incident Response Team) to deal with security incidents effectively.

The categorisation of incidents under this provision is explained in ***Annex One*** of this Regulation.

<u>Article 29:</u> Sharing information on Security Incident

The Licensee and/or any service provider interfacing with the licensee shall immediately share with the Regulatory Authority any security incidents which have occurred and considered as critical or major as defined in ***ANNEX ONE*** of this Regulation within 24 hours of the incident(s) occurrence using E-mail specified by the Regulatory Authority.

Initial notifications of "urgent incidents" shall be made by licensee within three (3) hours of incident(s) through the E-mail of the Regulatory Authority.

(j) au rapport mensuel pour l'analyse des causes profondes;
(k) à la création d'une équipe interne de gestion des incidents pour travailler en collaboration avec la CSIRT (Computer Security Incident Response Team) du gouvernement afin de traiter efficacement les incidents de sécurité.

La catégorisation des incidents au titre de cette disposition est reprise à l'***Annexe Premier*** du présent règlement.

<u>Article 29:</u> Echange d'information sur l'incident de sécurité

Le titulaire de licence et/ou tout fournisseur de services œuvrant avec le titulaire de licence doit immédiatement déclarer à l'Autorité de Régulation tout incident de sécurité qui s'est produit et qui est considéré comme critique ou majeur tel que défini à l'***ANNEXE PREMIER*** du présent règlement dans les 24 heures suivant l'incident par l'adresse électronique spécifié par l'Autorité de Régulation.

Les notifications initiales des « incidents urgents » doivent être faites par le titulaire de licence dans les trois (3) heures suivant l'avènement de l'incident, à travers l'adresse électronique de l'Autorité de Régulation.

Uwahawe uruhushya agomba gutanga raporo ku bibazo bicirirtse n'ibito buri kwezi abinyujije mu nzira z'itumanaho koranabuhanga zagenwe n'Urwego Ngenzuramikorere.

The licensee must submit reports of moderate and minor incidents, on a monthly basis through electronic communication channels prescribed by the Regulatory Authority.

Le titulaire de licence doit soumettre le rapport d'incidents modérés et mineurs, sur une base mensuelle à travers des chaînes de communication électroniques approuvés par l'Autorité de Régulation.

Urwego ngenzuramikorere rumenyeshwa ibibazo byose hakoreshwa ifishi y'ibibazo iri ku ***MUGEREKA WA II*** w'aya mabwiriza.

The Regulatory Authority shall be notified of all incidents report through the form contained in ***ANNEX II*** of this regulation.

L'Autorité de Régulation doit être notifiée des rapports de tous les incidents à travers la fiche figurant à l'***ANNEXE II*** du présent règlement.

Urwego Ngenzuramikorere rusesengura ibyo bibazo kandi rugakora ku buryo ayo makuru akoreshwa n'uwahawe uruhushya n'izindi nzego zibifitiye ububasha kugira ngo hirindwe ko ibibazo nk'ibyo byongera kuvuka mu gihe kiri imbere.

The Regulatory Authority shall assess such incident(s) and ensure that this information is utilized by the licensee and other competent organs to avoid future occurrence of similar incidents.

L'Autorité de Régulation évalue ces incidents et s'assure que ces informations sont utilisées par le titulaire de licence et d'autres organes compétents pour éviter les incidents similaires dans le futur.

<u>Ingingo ya 30</u>: Ikurikirana n'iyubahirizwa ry'ibisabwa

<u>Article 30</u>: Monitoring and Compliance

<u>Article 30</u> : Surveillance et conformité

Uwahawe uruhushya wese agomba gukurikirana no kubahiriza ibipimo ngenderwaho mu by'umutekano avugwa muri aya mabwiriza mu rwego rwo kugira imiyoboro na serivise bitekanye bitekanye.

The Licensee shall monitor and comply with all security standards provided for under this regulation to maintain secured networks, systems and services.

Le titulaire de licence doit surveiller et respecter toutes les normes de sécurité prévues par le présent règlement pour garder les réseaux, les systèmes sécurisés et les services.

Urwego Ngenzuramikorere rukora amagenzura yo kureba ko aya mabwiriza yubahirizwa rimwe mu mwaka cyangwa ikindi gihe cyose bibaye ngombwa.

The Regulatory Authority shall conduct audits for compliance with this Regulation on annual basis or at a time when need arises.

L'Autorité de Régulation effectue des audits pour assurer la conformité au présent règlement sur une base annuelle ou chaque fois que le besoin de présente.

Ingingo ya 31: Gutanga raporo

Raporo zose z'amasuzuma, iz'ubugenzuzi n'iza gahunda kimwe na raporo ku bibazo zishyikirizwa Urwego Ngenzuramikorere mu buryo bwagenwe no mu gihe kivugwa muri aya mabwiriza.

Urwego Ngenzuramikorere rushobora guhindura uburyo bwo gutanga raporo igihe rubishakiye n'umurongo uwahawe uruhushya anyuzaho ibibazo byerekeye umutekano w'umuyoborobyavutse.

UMUTWE WA VI: IBIHANO BYO MU RWEGO RW'UBUTEGETSI

Ingingo ya 32: Kutubahiriza inyandiko itegeka ibigomba kubahirizwa mu bijyanye n'umutekano w'imiyoboro

Uwahawe uruhushya wese utubahiriza icyemezo kihanangiriza gitangwa n'Urwego Ngenzuramikorere hakurikijwe ibiteganywa n'aya mabwiriza ahanishwa ihazabu yo mu rwego rw'ubutegetsi iri hagati y'amafaranga y'u Rwanda miliyoni imwe (1.000.000) na miliyoni eshanu (5.000.000).

Iyo atubahirije icyemezo cyihanangiriza ahanishwa ihazabu yo mu rwego rw'ubutegetsi y'inyongera ingana n'amafaranga y'u Rwanda ibihumbi magana

Article 31: Reporting

All assessments, audit and plan reports shall be submitted to the Regulatory Authority in prescribed manner within the time limit specified in this regulation.

The Regulatory Authority may at any time determine the audit format and communication channel through which security incidents will be reported by the licensee.

CHAPTER VI: ADMINISTRATIVE SANCTIONS

Article 32: Non-Compliance with the Network & Systems Security Enforcement Notice

Any Licensee who does not comply with the enforcement notice issued by the Regulatory Authority in accordance with the provisions of this Regulation shall be liable to an administrative fine of one million (1,000,000) and five million (5,000,000) FRW.

Failure to comply with the enforcement notice shall incur an additional administrative fine of five hundred thousand (500,000) FRW francs

Article 31 : Rapports

Toutes les évaluations, les rapports d'audit doivent être soumis à l'Autorité de Régulation de la manière prescrite et dans les délais spécifiés dans le présent règlement.

L'Autorité de Régulation peut à tout moment déterminer le format d'audit et le canal de communication à travers lesquels les incidents sont signalés par le titulaire de licence.

CHAPITRE VI: SANCTIONS ADMINISTRATIVES

Article 32: Non-respect de la mise en demeure pour la sécurité des réseaux et des systèmes

Tout titulaire de licence qui ne se conforme pas à la mise en demeure émise par l'Autorité de Régulation conformément aux dispositions du présent règlement est passible d'une amende administrative comprise entre un million (1.000.000) et cinq millions (5.000.000) FRW.

Le non-respect de la mise en demeure entraîne une amende administrative supplémentaire de cinq cent mille FRW (500.000) par jour,

atanu (500.000) buri munsi abarwa uhereye igihe yakiriye icyo cyemezo kihanangiriza.

per day as calculated from the date of receipt of the concerned enforcement notice.

calculée à compter de la date de réception de la mise en demeure concernée.

Ingingo ya 33: Kudashyira mu bikorwa ingamba z'umutekano

Uwahawe uruhushya udashyira mu bikorwa ingamba z'umutekano za ngombwa mu rwego rwo kurinda kirogoya muri serivisi z'abafatabuguzi ahanishwa ihazabu yo mu rwego rw'ubutegetsi iri hagati y'amafaranga y'u Rwanda miliyoni imwe (1.000.000) na miliyoni eshanu (5.000.000).

Iyo akomeje kudashyira mu bikorwa ingamba z'umutekano ahabwa ibihano by'inyongera bishobora no gutuma yamburwa uruhushya.

Article 33: Failure to Implement Security Measures

Any licensee who fails to implement the relevant security measures to avoid interruption of subscribers' services shall be liable to an administrative fine between one million (1,000,000) and five million (5,000,000) FRW.

Continuous failure to implement the security measures shall incur extra sanctions that may lead to revocation of the license.

Article 33: Non-exécution des mesures de sécurité

Tout titulaire de licence qui ne parvient pas à faire appliquer les mesures de sécurité pour éviter l'interruption des services des abonnés est passible d'une amende administrative comprise entre un million (1.000.000) et cinq millions (5.000.000) FRW.

L'incapacité prolongée de faire appliquer les mesures de sécurité entraîne les sanctions supplémentaires pouvant entraîner la révocation de la licence.

Ingingo ya 34: Kwanga gutanga amakuru arebana n'ibibazo by'umutekano

Uwahawe uruhushya udatanga cyangwa wanga gutangira igihe amakuru arebana n'ikibazo cy'umutekano cyangwa agaha amakuru atuzuye cyangwa y'ibinyoma Urwego Ngenzuramikorere cyangwa ntatange amakuru arebana n'ibibazo by'umutekano mu buryo bwagenwe cyangwa mu gihe cyagenwe, ahanishwa ihazabu yo mu rwego rw'ubutegetsi iri hagati y'amafaranga y'u

Article 34: Refusal to Provide Information Related to Security Incidents

Any licensee who fails or refuses to provide timely the information related to security incident or gives partial or false information related to the security incidents to the Regulatory Authority or fails to provide information related to security incident in accordance with the relevant procedure or within the planned timeframe, shall be liable to an administrative fine of between five

Article 34: Refus de fournir les informations liées aux incidents de sécurité

Tout titulaire de licence qui omet ou refuse de fournir en temps exigé les informations liées à l'incident de sécurité ou donne des informations incomplètes ou fausses liées aux incidents de sécurité à l'Autorité de Régulation ou omet de fournir des informations liées à l'incident de sécurité conformément à la procédure y relative ou dans les délais prévus, est passible d'une amende administrative comprise entre cinq

Rwanda ibihumbi magana atanu (500.000) na miliyoni imwe (1.000.000).

hundred thousand (500,000) and one million (1,000,000) FRW.

cent mille (500.000) et un million (1.000.000) FRW.

Ingingo ya 35: Gutinda gutanga raporo

Article 35: Delay to Submit the Reports

Article 35 : Retard de présenter les rapports

Uwahawe uruhushya, ku bushake cyangwa ku burangare, udaha Urwego Ngenzuramikorere raporo ya gahunda, raporo y'ubugenzuzi na gahunda yo gukosora inenge nk'uko biteganywa n'aya mabwiriza ahanishwa ihazabu yo mu rwego rw'ubutegetsi iri hagati y'amafaranga y'u Rwanda ibihumbi magana abiri (200.000) na miliyoni imwe (1.000.000).

Any licensee who intentionally or by negligence fails to submit the audit plan report, the audit report and remediation plan to the Regulatory Authority as provided under this Regulation shall be liable to an administrative fine of between two hundred thousand (200,000) and one million (1,000,000) FRW.

Tout titulaire de licence qui, intentionnellement ou par négligence, ne soumet pas le rapport du plan d'audit, le rapport d'audit et le plan de correction à l'Autorité de Régulation conformément au présent règlement est passible d'une amende administrative comprise entre deux cent mille francs Rwandais (200.000) et un million (1.000.000) FRW.

Ingingo ya 36: Kutubahiriza igisabwa icyo ari cyo cyose giteganijwe n'aya mabwiriza

Article 36: Non-Compliance to any Requirement of this Regulation

Article 36: Non-respect de n'importe quelle provision du présent règlement

Uwahawe uruhushya utubahiriza ibindi byose bisabwa n'aya mabwiriza ahanishwa ihazabu yo mu rwego rw'ubutegetsi iri hagati y'amafaranga y'u Rwanda miliyoni imwe (1.000.000) na miliyoni eshanu (5.000.000).

Any Licensee who does not comply with any other requirement of this Regulation shall be liable to an administrative fine of between one million (1,000,000) and five million (5,000,000) FRW.

Tout titulaire de licence qui ne se conforme pas à toute autre provision du présent règlement est passible d'une amende administrative comprise entre un million de francs Rwandais (1.000.000) et cinq millions (5.000.000) FRW.

Ingingo ya 37: Ibihano by'inyongera

Article 37: Additional Sanctions

Article 37 : Sanctions supplémentaires

Urwego Ngenzuramikorere rufite ububasha bwo gutanga ibihano by'inyongera hakurikijwe amategeko n'amabwiriza abigenga igihe rusanze ari ngombwa.

The regulatory Authority reserves the power to impose additional sanctions in accordance with applicable laws and regulations when deemed necessary.

L'Autorité de Régulation se réserve le pouvoir d'imposer des sanctions supplémentaires conformément aux lois et règlements en vigueur lorsqu'elle le juge nécessaire.

UMUTWE WA VII: INGINGO ZISOZA

Ingingo ya 38: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza

Ingingo zose z'amabwiriza abanziriza aya kandi zinyuranyije na yo zivanyweho.

Ingingo ya 39: Igihe aya mabwiriza atangira gukurikizwa

Aya Mabwiriza atangira gukurikizwa ku munsi ashyiriweho umukono na Perezida w'Inama Ngenzuramikorere.

Bikorewe i Kigali ku wa 29/05/2020

(sé)

Dr Ignace GATARE

Perezida w'Inama Ngenzuramikorere

CHAPTER VII: FINAL PROVISIONS

Article 38: Repealing Provision

All prior regulatory provisions contrary to this regulation are hereby repealed.

Article 39: Commencement

This Regulation shall come into force on the date of its signature by the Chairperson of the Regulatory Board.

Done at Kigali on 29/05/2020

(sé)

Dr Ignace GATARE

Chairperson of the Regulatory Board

CHAPITRE VII: DISPOSITIONS FINALES

Article 38: Disposition abrogatoire

Toutes les dispositions antérieures contraires au présent règlement sont abrogées.

Article 39 : Entrée en vigueur

Le présent Règlement entre en vigueur à la date de sa signature par le Président du Conseil de Régulation.

Fait à Kigali le 29/05/2020

(sé)

Dr Ignace GATARE

Président du Conseil de Régulation

ANNEX ONE: MANAGEMENT OF INCIDENTS

Incident Metrics			
	Core Network Services	VAS	Non-Urgent Services
Entire Network	Critical	Critical	Major
Partial Network	Critical	Major	Moderate
Individual	Moderate	Minor	Minor

Seen to be attached to the Regulation N° 010/R/CR-CSI/RURA/020 of 29/05/2020 governing Cybersecurity

(se)

Dr Ignace GATARE

Chairperson of the Regulatory Board

ANNEX II: SECURITY INCIDENT RESPONSE FORM

The following is a sample incident report form. The report is an example of the types of information and incident details that will be used to track and report security incidents to RURA.				
Contact Information				
1.	**Company Name**			
2.	**Last Name**		**First Name**	
3.	**Job Title**		**Mobile No**	
4.	**Email:**			
Incident General Information				
5.	**Type/Name of Incident**			
6.	**Brief description of incident**			
7.	**Date/Time of Incident Detection/Occurrence**		**Time:**	**Date:**
8.	**Site/Location**			
9.	**Date and time of Resolution**			
10.	**Known Impact**			
11.	**Confidential/Personal Identifiable Information Affected**		☐ **Yes** ☐ **No**	
12.	**Systems and Services Impacted**		**Service(s) affected**	
			Number/proportion of users affected	
			Networks & assets affected	
13.	**Severity Level**		**Critical** ☐	**Major** ☐
			Moderate ☐	**Minor** ☐
14.	**Summary of incident cause and action taken so far**			
15.	**Source of Incident**		**Description:**	
			Internal ☐	**External** ☐
16.	**Third party details [*If the cause of the incident was the failure of a third-party service]***			
17.	**Name and contact details for follow up *[If different from above*]**			

Incident Mitigation	
Status	
Timeline	
Comments	
Comments	**Additional Comments/Notes/Recommendation**
[Any additional notes, Follow-on actions recommended to be taken, information or observations related to the security incident or this report.]	

Seen to be attached to the Regulation N° 010/R/CR-CSI/RURA/020 of 29/05/2020 governing Cybersecurity

(se)

Dr Ignace GATARE

Chairperson of the Regulatory Board