



Business Rules for the Registration of Communications Subscribers Regulations

August 2026

CONTENTS

PART I: GENERAL	6
INTRODUCTION:	6
OBJECTIVE:	6
SCOPE:	6
GENERAL RULES	7
COMMISSION's DISCRETIONARY POWERS	13
PART II: BUSINESS RULES - SIM REGISTRATION	14
A. HARMONIZATION OF DEMOGRAPHICS AND BIOMETRICS RECORDS FOR AN EXISTING SUBSCRIBER	14
2.1. Demographics are mismatched and require update	14
2.2. NIMC Biometrics do not match with SIM Registration Record. Complete KYC Update Required	16
2.3. NIN Linking and Harmonization for Nigerians in the Diaspora	18
B. EXISTING CORPORATE SUBSCRIBER - HARMONIZATION OF NIMC AND SIM REGISTRATION DATABASE	19
2.4. Corporate Subscriber Harmonization of NIMC and SIM Registration Database (Corporate & IOT/M2M)	19
2.5. Corporate Demographic and Biometric Mismatch - Consent via USSD For NIN- SIM Registration Update	19
2.6. Corporate Demographic and Biometric Mismatch - Consent via Physical Process for NIN- SIM Registration Update	21
2.7. Subscriber Consent via SMS for SIM Registration KYC Update with NIN Records (Corporate & IOT/M2M)	22
2.8. Subscriber Consent via COMMUNICATIONS SERVICE PROVIDER's Website for SIM Registration KYC Update with NIN Records (Corporate & IOT/M2M)	23
2.9. Subscriber Consent via Email for SIM Reg. KYC Update with NIN Records (Corporate & IOT/M2M)	24

c. NEW SIM REGISTRATION/ACTIVATION FOR INDIVIDUALS, CORPORATES AND MACHINE-TO-MACHINE.....25

NEW SIM REGISTRATION/ACTIVATIONS FOR INDIVIDUALS 25

2.10. Subscriber Acquisition (SIM Sales) Process	25
2.11. New Subscriber Acquisition with NIN (SIM Sales)	25
2.12. New SIM Acquisition/SIM Sales Business Guidelines.....	25
2.13. Existing Subscriber with NIN.....	26
2.14. New and Existing Subscriber (Foreigners) SIM Acquisition/Activations	27
2.15 Subscriber Acquisition and SIM Sales Process (Corporate & IoT/M2M Subscribers).....	32
2.16. New SIM Registration/Activation Business Guidelines (Corporate & IOT/M2M)	32
2.17. Existing Subscribers with NIN (Corporate & IOT/M2M)	34
2.18. DIPLOMATIC MISSIONS AND EMBASSIES	36

PART III. MOBILE NUMBER PORTABILITY (MNP) INDIVIDUALS AND CORPORATE SUBSCRIBERS.....37

3.0 Individual Subscribers with NIN requesting Mobile Number Porting (MNP).....	37
3.1 New Subscribers with NIN requesting Mobile Number Porting (MNP) (Corporate& IOT/M2M)	38
3.2 Existing Subscribers with NIN requesting Mobile Number Porting (MNP) (Corporate & IOT/M2M)	39

PART IV: CHURN AND RECYCLING OF SUBSCRIBER SIM ACTIVATION.....41

4.0 Churned and Recycled SIM Activation	41
4.1 Churned and Recycled SIM Activation for Foreigners	42
4.2 Recycling (Corporate & IOT/M2M)	43
4.3 Policy on Inactive Account Management and Churn.....	44

PART V: PROCESS FLOW FOR NON-GSM, PNLs & ISPs45

5.1 Physical: New Customer (Corporate) Seeking to Purchase Non-GSM/PNL/ISP Services.....	45
5.2 Physical: Call Center Licensee Seeking to Purchase Non-GSM /PNL Services.....	46
5.3 Physical. New Customer (Individual) Seeking to Purchase PNL/ISP Services.....	47
5.4 Online New Customer (Individual) Seeking to Purchase PNL/ISP Services.....	47
5.5 Online New Customer (Corporate) Seeking to Purchase Non-GSM /PNL/ISP Services.....	48
5.6 Online Call Center Licensee Seeking to Purchase Non-GSM /PNL	

Services.....	49
5.7 Online KYC 3rd Party Onboarding Process for Call Center Licensees.....	50
5.8 Rules for Non-GSM/ISP/PNL Online KYC	50
5.9 KYC Documents Requirements	51
PART VI: GOVERNANCE	52
6.1 Governance for Agents and Device handlers	52
PART VII: SIM REGISTRATION RESTRICTION	54
7.1 SIM Registration Restriction.....	54
PART VIII: MSISDN BLOCKING, BLACKLISTING AND ACCESS LIMITATIONS FOR PERSONS AND AGENTS.....	56
8.1 Registered SIMs Suspected.....	56
8.2 Registered SIMs fraudulently registered.....	57
8.3 Fraudulent MSISDN SIM Suspected.....	57
8.4 Fraudulent MSISDN SIM used.....	58
8.5 Blacklist of persons/Agents.....	59
8.6 Restrictions for persons under investigation.....	59
APPENDIX 1 REQUIREMENTS OF THE SELF SERVICE KNOW YOUR CUSTOMER (KYC) SYSTEM.....	61
APPENDIX 2 GLOSSARY OF TERMS AND ABBREVIATIONS	64
APPENDIX 3: SERVICE LEVEL REQUIREMENT WITH NIMC AND LIMITEDSERVICE OFFERINGS TO SUBSCRIBERS.....	66
APPENDIX 4: COMMUNICATIONS SERVICE PROVIDER SERVICE LEVEL REQUIREMENT.....	67
APPENDIX 5: CONSENT RULES.....	72
APPENDIX 6: SAMPLE MESSAGES -USSD.....	73
APPENDIX 7: NIMC AGREED AND APPROVED MINIMAL DATA FIELDS...74	
APPENDIX 8: REQUIRED LIVENESS DETECTION AND FACIAL IMAGE STANDARDS.....	77

Document History

Date	Version
August 2022	First Issuance
April 2024	First Amendment
August 2026	Second Amendment

PART I: GENERAL

INTRODUCTION

This Business Rules is issued pursuant to the Registration of Communications Subscribers Regulations to provide specifications for SIM registration and verification/validation through the mandatory use of a National Identity Number (NIN). Accordingly, and given how the use of NIN has become integral in the authentication of identity in the Communications sector, this document sets out the Business Rules and operational processes that will govern the following contexts:

1. SIM registration and activation for new & existing subscribers (individuals and corporates)
2. Identity verification and validation through NIMC as part of the activation process of SIM after registration.
3. SIM registration, verification and activation for foreigners
4. Mobile Number Portability (MNP)

OBJECTIVE

This document sets out the Business Rules for implementation of the Registration of Communications Subscribers Regulations 2022 for SIM Card Registration and related activities within the context of the Nigerian Communications sector. The objectives of the Business Rules are as follows:

- Harmonization of NIN and SIM Registration Data to improve the integrity of the SIM Registration Database.
- Providing operational guidance for contexts and scenarios to ensure standardized implementation of the provisions of the Registration of Communications Subscribers Regulations 2022 for SIM Registration.
- Specifying processes required to give effect to the provisions of the Registration of Communications Subscribers Regulations 2022 for SIM Card Registration and related activities.
- Elimination of existing system and process gaps that facilitate improper SIM registration and other fraudulent SIM -related practices in the Nigerian Communications Industry.
- Institution of processes that will guarantee a secure, sustainable and scalable mechanism of registering and verifying citizens' and flexibly utilizing same for various approved purposes.

SCOPE

The Business Rules shall apply to processes impacted by SIM Registration requirement which include but not limited to the following:

1. NIN-SIM Registration Database Harmonization.
2. New SIM registration and Activation by the Service Providers.
3. Verification and validation of identity through NIMC as part of the SIM activation process.
4. SIM registration and Activation for foreigners
5. Mobile Number Portability
6. Churned and Recycled SIMs
7. Agents and Dealers Governance

GENERAL RULES

1. NIMC Database is the reference database for Identity Management and verification/validation during SIM Registration for the relevant business processes within the communications industry.
2. Subscriber Registration shall be the sole duty of the Nigerian Communications Commission and shall consist of the following:
 - Collection of Subscriber information,
 - Registration of the subscriber with applicable registration reference, and
 - Activation of subscription after successful NIN verification.
3. Subscriber Identity verification shall be carried out by NIMC and shall consist of the verification of the subscriber using their NIN in accordance with NIN policy.
4. Basic NIN verification (NIN only) shall be allowed pending when NIMC database capacity is optimized.
5. Subject to the Business Rules on foreigner SIM activations, the NIN is the only acceptable proof of Identity for customers seeking to subscribe to Communications services.
6. Communications Service Providers and their dealers or agents shall ensure that every subscriber has only one NIN and no registration shall be conducted for any subscriber with more than one NIN.
7. Where a subscriber presents a NIN as proof of Identity, the Communications Service Provider shall utilize the online NIMC NIN – Verification Service to confirm and authenticate such identity based on the rules defined herein.
8. Subscriber records on SIM Registration Database must align with the records on the National Identity Mandatory Database. As a result, any alteration to subscriber data must occur on NIN database prior to an update to SIM Registration records.
9. The use of NIN is Mandatory for all SIM Activations and, MNP.
10. The use and capture of other forms of identification is not mandatory except in the case of subscribers exempted from enrolling for NIN.
11. SIM activations for foreigners exempted from enrolling for NIN shall be configured for a period of 2 weeks/1 month/3 months as applicable to the Visa validity and can be renewed further upon request and where the visa is not for a stay of 2 years and above.
12. Communications Service Providers shall utilize all Foundational data from NIMC database as SIM Registration details per subscriber as part of the harmonization process, new SIM activations and MNP.

13. Every new line acquired by the subscriber shall have no access to a Licensee's network service prior to activation; save for the ability to receive Short Message Service from the Licensee.
14. Every activated line (new registration must carry out a Revenue Generating Event (RGE) within 48-hours of activation and another RGE within the next 48 hours (96th Hour).
15. For every new registration, a SMS notification message should be sent to all of the subscriber's numbers on the MNO's network (where applicable).
16. Subject to the Nigerian Data Protection Act 2023, the Consumer Code of Practice Regulations on data privacy and any other regulatory instrument issued by the Commission on data privacy from time to time, Communications Service Providers shall retain subscriber information including but not limited to biodata, facial image for business activities other than SIM activation and MNP.
17. For effective verification of NIN, subscriber biometrics data including but not limited to facials, fingerprint or any other biometrics approved by the NCC shall be utilized subject to data privacy rules and NIMC's supporting infrastructure.
18. For verification of NIN carried out using subscriber facial image, the Facial Verification shall be done electronically and subsequently via case-management which includes manual facial verification (eyeballing). The commencement of full compliance with electronic matching for facial verification shall be ascertained by thresholds and standards set out and determined by the NCC. Note that the following standard set will apply:

The similarity percentage is categorized into the following tiers:

☐ Above 80%:	i. The uploaded image matches the NIN image with a high degree of accuracy.	Action: The Communication Service Provider can proceed with customer registration confidently.
☐ Between: 70% - 79%:	management is further divided into two tiers for better case i. ii. Minor (75% - 79%): The similarity is close to acceptable, but Communications Service Providers are advised to review the data manually before proceeding. Major (70% - 74%): There is a noticeable disparity in the images. Communications Service Providers should conduct a more thorough investigation before deciding on registration.	Action: Case Management; When the match is moderate, and further scrutiny is advised.

□ Below 70%:	i. The uploaded image does not sufficiently match the NIN image.	Action: Communications Service Providers are strongly advised not to proceed with registration for security and compliance reasons.
---------------------	--	---

19. All NCC licensed operators, technology partners and biometric partners shall be expected to abide strictly in compliance with the standards under Appendix 8 of these business Rules and as may be determined by the NCC.
20. Adequate quality assurance measures shall be built into the validation and verification processes to ensure accuracy of validations and verifications.
21. All subscribers with Bank Verification Number (BVN) generated NIN shall be required to update their biometrics at NIMC offices before such NIN can be used by Communications Service Providers for verification, linkage and other SIM related transactions.
22. Where BVN generated NIN is flagged by NIMC, Communications Service Providers shall not conduct sale of New SIM and MNP for Individual and Corporate (IoT/M2M) subscriber. Communications Service Providers shall advise the Subscriber to return to NIMC office for regularization;
23. Subscriber's consent shall be required prior to the harmonization and updating of the individual and corporate subscriber's SIM registration data record with NIMC data record. Subscriber Consent Channels set out in **Appendix 5** shall apply;
24. In the case of SIM registration harmonization for existing subscribers, where biometric details need to be updated or harmonized, the subscriber may be required to physically visit the Communications Service Providers' store; while in certain instances the Communications Service Providers may rely on self-service processes that are set up in line with the provisions of these Business Rules
25. In the case of SIM registration harmonization for existing Corporate subscribers, effective verification of Primary Telecom Master shall be done by electronic facial verification and case management which includes manual facial verification (eye-balling) of the Primary Telecom Master's passport photograph and verification form vis a vis the NIN details of the Primary Telecom Master from the NIMC database;
26. E-mails shall be sent to the official e-mail address of the authorized Primary or Secondary Telecom Master in cases of mismatched biometrics and/or demographic details of the corporate subscriber;
27. Physical consent forms shall be signed by the Primary Telecom Master only. The signature of the Secondary Telecom Master or any other party shall not suffice for this purpose;
28. Consent via portal, or any other channel, shall be given by Primary Telecom Master only;
29. All Communications Service Providers SIM Registration data (demographics and verified biometrics) shall be transmitted to NCC Central Database for storage in the interim until the NCC New Data Dictionary is issued;
30. For New SIM Acquisition/Activation and MNP, Communications Service Providers shall capture live image or fingerprints as evidence of biometric detail;

31. Where Communications Service Providers are unable to successfully verify the subscriber's NIN records due to a degradation in the service availability threshold, Communications Service Providers are to refer to Appendix 3 and 4 to this Business Rules.
32. Electronic Image Matching shall replace manual backend facial verification (eyeballing) when available to improve accuracy of Communications Service Providers image matching process against NIMC database and SIM Registration database. However, manual verification will still be required in cases where Facial image system cannot be match;
33. It shall be possible to identify number of SIMs allocated to a subscriber per Communications Service Providers and across Communications Service Providers;
34. Record of all recycled SIMs shall be purged of any NIN attached, this is to allow New subscriber register or submit and link a new NIN;
35. In respect of Foreigners who wish to activate New SIM (which includes subscription medium), and perform MNP (porting of numbers), the following general rules shall apply:
 - a) Foreigners who are lawfully residing in Nigeria for a period of two years or more fall under the category of Registrable persons and shall require a NIN to register their SIM and request for MNP;
 - b) Foreigners validly transiting through Nigeria or are employed in or reside in Nigeria for less than 24 months are exempted from the mandatory use of NIN requirement. Persons in this category need to provide justification that they will be residing in Nigeria for less than 2 years;
 - c) NIN is mandatory for Foreigners with legal residency status or those living in Nigeria for 2 years and above. For those who do not already have a NIN, Communications Service Providers shall capture the Resident's details for NIN issuance as part of the NIN enrolment process, upon presentation of residents permits;
 - d) Foreigners with Visitor's visas (with visa less than 2 years) do not require a NIN. Communications Service Providers will capture the following on their records prior to New SIM activations and MNP: International passport biodata page; and Visa page.
 - e) Foreigners with Diplomatic visas (including family diplomatic visas) will also require a NIN for their personal telephone lines if they are staying in Nigeria for 2 or more years.

Those staying less than 2 years will require the following for registration of their personal telephone lines;

 - i. International passport biodata page
 - ii. Letter from embassy indicating that their stay is for less than 2 years;
36. In respect of Embassies and Diplomatic Mission the following rules shall apply:
 - a) The data page containing the passport number of the diplomatic passport of the Head of Mission/Embassy along with a Letter of Request signed by the Ambassador or its equivalent for registration of the official telephone lines of the Embassy/Mission in Nigeria shall be submitted to the Ministry of Foreign Affairs for verification and confirmation and registration of the SIMs;
 - b) For the registration of SIM (which includes subscription medium) of Diplomatic Missions, the following are required:
 - i. The Data page containing the passport number of the Diplomatic Passport of the Head of Mission/Embassy.

- I. A Letter of Request signed by the Ambassador or its equivalent.
- II. Letter verifying and confirming registration of SIMs by the Ministry of Foreign Affairs.
- IV. Any Foreign member of a Diplomatic Mission requiring SIMs for personal use shall go through the processes under item 4 or 8 above;

37. The following are general rules that shall apply to Corporate and IOT/M2M new SIM sales/activation:

- a) Primary Telecoms Master (TELECOM MASTER) shall be minimum Executive Management Staff.
- b) Corporate subscribers have the option of also appointing a Secondary or Operations Telecoms Master.
- c) Both Primary & Secondary/Operations Telecoms Master shall be indicated in a TELECOM MASTER Authorization letter.
- d) IOT/ M2M SIM registrations will only require NIN of the Primary Telecom Master. The NIN data for the Primary number is linked to all other numbers within the same account.
- e) SIM Security Protocols would be implemented on the IOT/M2M SIM profile to ensure that the SIMs can only be used for point-to-point Data services – specific to the URL they are working with. All other services will be barred.
- f) Telecoms Master Authorization Letter shall be signed by 1 or 2 C-Level staff (or above) of the Corporate Organization Telecoms Master Authorization Letter shall provide:
 - i. Registered names of the Primary Telecoms Master
 - ii. Official Designation of the Primary Telecoms Master
 - iii. NIN of the Primary Telecoms Master i.e. Primary NIN
 - iv. MSISDN of the Primary Telecoms Master (within the corporate account)
 - v. Registered names of the Secondary/Operations Telecoms Master (Optional) vi. Official Designation of the Secondary/Operations Telecoms Master
 - vii. MSISDN of the Secondary/Operations Telecoms Master (within the corporate account)
 - viii. NIN of the Secondary Telecom Master.
 - ix. Indemnity letter specifying the full responsibilities and liabilities of the Primary Telecoms Master and signed by the Primary Telecoms Master and C-Level staff of the Corporate Organization.
 - x. A CSV file (or other searchable format) of all associated/secondary SIMs on the same account is provided (not applicable for IOT/M2M). This shall provide:
 - All associated SIMs on the account.
 - First, Middle (optional) and Last Names of each Secondary User
 - NIN of each Secondary user i.e. Secondary NIN
 - Alternate SIMs of Secondary Users

- Certificate of Incorporation with Registration Number duly verified by CAC (not applicable to companies listed on Nigerian Stock Exchange)
- Tax Clearance Certificate or Tax Identification Number (not applicable to companies listed on Nigerian Stock Exchange)
 - i. Public sector and Government organizations to present Legal Instrument showing evidence of establishment.
 - ii. Verify Primary Telecom Master NIN by matching Communications Service Providers Primary Telecom Master SIM Registration with NIMC records of Primary Telecom Master NIN.
 - iii. Where there are mismatches or Primary Telecom Master SIM Registration is unavailable in respect of an Existing Corporate Subscriber, Communications Service Providers shall obtain Primary Telecom Master Passport Photograph and other demographic details.
 - iv. Communications Service Providers shall verify Primary Telecom Master NIN records against details provided via the electronic facial matching and case-management which includes manual facial verification process.
 - v. Communications Service Providers shall provide NIMC records to Primary Telecom Master And obtain consent to use the records as Corporate SIM Registration.
 - vi. Communications Service Providers shall update Primary Telecom Master SIM Registration with NIMC records; store consent, passport photo and all other documents on the account.
 - vii. Communications Service Providers shall validate the Secondary NIN of the Corporate. This shall not be applicable for IOT/M2M;
 - viii. Communications Service Providers shall copy verified Primary Telecom Master NIN and each validated Secondary NIN on the SIMs accordingly;
- 34. Where a Data only service is particular to individual use e.g. Home, car tracking, Wi-Fi, MiFi services, et al, the standard NIN registration process will apply;
- 35. Where Primary Telecom Master's NIN data and Communications Service Providers SIM Registration records match, and Secondary Telecom Master's NIN is successfully verified, other forms of verification shall not be required;
- 36. Where Primary Telecom Master's NIN data and Communications Service Providers SIM Registration KYC records do not match (or where Primary Telecom Master's SIM Registration database is not available), SIM Registration data shall be updated with NIN details upon facial verification of Primary Telecom Master's passport photograph and consent form from Corporate subscriber;
- 37. Any peculiar request different from any Corporate entity which is at variance to the General Rules on Corporate and IoT/M2M SIM activation shall be treated on case by case basis after such Corporate entity procures a waiver from NCC and upon written directives from the NCC to the concerned Communications Service Providers.
- 38. A check must be carried out by the Communications Service Providers for all new activations and Port-in requests to ensure that the limit on the number of activations per subscriber as specified by the Commission from time to time are strictly adhered to.
- 39. The total number of SIMs an individual subscriber is permitted to acquire on any Communications Service Providers' network shall be as determined by the Commission at any given period. This limit shall not apply to Corporate and IoT/M2M Activation scenarios.

40. The self-service option for resolving biometric mismatches in Sections 2.2, 2.3 and 2.4 below can only be conducted by the Communications Service Provider itself and cannot be an option for such activity by an agent or third party.
41. All self-service activities shall be in line with the specifications and requirements set out in Appendix 1 of these Business Rules.
42. Agents, third parties and other entities are not allowed to use the self-service option for any service, mismatch resolution or data update. These category must conduct these activities in a controlled environment.
43. A Controlled environment for the purposes of these Business Rules must have the following features
 - i. The environment must be properly lit and illuminated
 - ii. Images should be captured against a white background
 - iii. The environment must have the logo of the Communications Service Provider
 - iv. The environment must be operated by a duly licensed and approved agent
 - v. The agent must have a valid means of identification and a verified NIN
 - vi. The registration center must be a permanent structure
 - vii. The premises must be clearly marked a “SIM Card Registration Centre”.
44. Communications Service Provider shall ensure Real-time SIM registration notifications are sent across all mobile networks to the registered NIN Subscriber devices.
45. Communications Service Providers shall ensure subscribers for self-service on their network have enabled the capability to check NIN-SIM linkage status across all networks.
46. Communications Service Providers shall ensure a controlled and simple NIN delinking process to address identified unauthorized or fraudulent SIM associations.
47. MSISDNs with no revenue generating event (RGE) for a continuous period of 365 days shall be delinked and barred in accordance with these Business Rules and any conditions the Commission may issue over time.

COMMISSION’S DISCRETIONARY POWERS/EXEMPTIONS

- All restrictions outlined in prior Registration policies above (daily caps, real-time requirements, etc.) are subject to modification or exemption at the sole discretion of the Nigerian Communications Commission (NCC).
- The NCC may approve deviations from these restrictions if deemed operationally expedient, necessary for public interest, or critical for National Security.
- NIN Exemptions/Waivers shall be considered by the Commission upon security clearance and grant of official approval.

PART II: BUSINESS RULES - SIM REGISTRATION

A. TRANSFER OF REGISTERED MEDIUM, HARMONISATION OF DEMOGRAPHICS AND BIOMETRICS RECORDS FOR AN EXISTING SUBSCRIBER

The following processes relating to the update and harmonization of SIM registration of existing subscribers with NIMC database shall be read and implemented in conjunction with the Paragraph 1 - General Rules, set out in this Business Rules.

2.1. Demographics are mismatched and require update		
2.1	Context and Rules	i. This is where a subscriber's biometric details (e.g. fingerprint or facial image) match with the NIMC database and SIM Registration database but the demographics of the subscriber in the NIMC database do not match with the demographic records in the SIM Registration database of the Communications Service Providers and therefore needs to be harmonized and updated as Functional Data for the Communications Service Providers use; ii. Verification of subscriber's NIN details on SIM Registration database shall be done using the biometrics of the subscriber (which includes facial image, fingerprints and any other biometrics approved by the NCC). iii. This can occur during the bulk verification and/or single verification of existing subscribers who have submitted their NINs for verification and linkage; iv. In this case, given that only demographic information needs to be harmonized, the subscriber shall not be required to physically visit the Communications Service Providers store. v. Where the source of mismatch is NIMC's database, subscriber shall be advised to visit NIMC's office for update. vi. This Rule can also apply to a SIM registered by a Parent/Guardian on behalf of a child or Ward while he was below 18 years and the Parents/Guardian wish to transfer the medium to the same child or ward when he is of age.
2.2	Mismatch Scenarios	The following mismatch or required change scenarios are contemplated under these Business Rules: i. Mismatched subscriber data; ii. Change of name due to

		marriage or any other circumstance; iii. Transfer of a medium registered by Parent for a child who has now attained the age of 18 years.
2.3	Harmonization Flow Summary	Where there is a mismatch, the following process shall apply: i. Validate and verify subscriber's NIN on NIMC database; ii. In the case of facial verification, Communications Service Providers will effectively verify the Subscriber's NIN data and match with SIM Registration using electronic Facial verification and case-management which includes manual facial verification (eyeballing); iii. The Communications Service Providers shall also require the subscriber to provide indemnification in the form of a Sworn Affidavit or Police report; iv. Validate whether NIMC Image & Live Image match; v. Trigger OTP to subscriber if transaction is a SIM Upgrade; vi. Obtain consent from subscriber via completed SIM Registration Form with Consent Note; vii. Copy NIMC Foundational Data and adopt as SIM Registration data; viii. Update subscriber's SIM Registration records with live image; ix. Save.

2.2 Others - NIMC Biometrics and Demographics do not match with SIM Registration Records Complete KYC Update Required

This flow covers below scenarios:

- A. Where a subscriber in possession of a line requests his/her SIM Registration data updated to reflect his/her NIN details.

	Context	i. This is where both the subscriber's NIMC biometrics (i.e., fingerprint or facial image) and demographic details do not match the data on the SIM Registration Database; ii. Effective Verification of subscriber's NIN details on SIM Registration database shall be done using the biometrics of the subscriber (which includes facial image and fingerprints). iii. Where there is a mismatch in biometric and demographic records between the NIMC and SIM Registration Database, Communications Service Providers shall also require the subscriber to provide indemnification in the form of a Sworn Affidavit or Police report;
		iv. This mismatch category requires the harmonization and update of the Subscriber's SIM Registration data with the NIMC foundational data (including biometrics) for the Communications Service Provider use; v. In this case, given that biometric update and harmonization is required, the subscriber may be required to physically visit the Communications Service Providers store or use the self-service option that may be provided for such resolution; vi. Where a customer is in possession of the line an OTP will be triggered should be used.
2.4	Mismatch Scenarios	The following mismatch scenarios are contemplated under these Business Rules: i. Child or ward (who was previously a minor and is now of age) in possession of a SIM originally purchased by living Parent or Guardian requesting that SIM Registration details be updated to his/her details. ii. Family member in possession of a SIM (who was previously a minor and is now of age) originally purchased by another living family member requesting that SIM Registration details be updated to his/her details.

2.5	Harmonization Flow Summary	Where there is a mismatch, the following process shall apply: - i Validate and verify NIN and biometrics of the Child (who was previously a minor and is now of age) and Parent or Guardian or Family member on NIMC database; - ii In the case of facial verification, Communications Service Providers will effectively verify the Subscriber's NIN data and match with SIM Registration using electronic Facial verification and case-management which includes manual facial verification (eye-balling); - iii The Communications Service Provider shall also require the subscriber to provide indemnification in the form of a Sworn Affidavit or police report; - iv Validate NIN Image & Live Image Match of both parties; - v Obtain consent from subscriber via completed SIM Registration Form with Consent Note. - vi SIM Registration Form will include Consent to update SIM Registration records NIMC; vii. The consent form will be signed by both Child (who was previously a minor and is now of age) and Parent to update SIM Registration record with NIMC Foundational data; viii. Trigger OTP to the line; ix. Copy NIMC Foundational data; x. Update SIM Registration records and biometrics; xi. xi Save.
-----	-----------------------------------	--

2.3 NIN Linking and Harmonization for Nigerians in the Diaspora

Context	The process relates to Nigerian citizen outbound roamers resident in the Diaspora and are constrained in the ability to enroll for NIN or update their NIN details (i.e. BVN generated NIN) due to prolonged spread of COVID-19 pandemic, lock-down measures put in place by countries to stave-off the spread of the COVID-19 pandemic, and the inadequate NIMC enrolment centers abroad.
NIN Linking and harmonization for Nigerians in diaspora	- i Communications Service Provider to identify and whitelist MSISDNs of all active Nigerian citizen outbound roamers on their respective network. - ii In determining the qualifying national/citizenship, Communications Service Providers will be guided by the nationality information previously provided by the subscriber at the point of SIM activation.
	- iii Communications Service Provider to send messages including but not limited to SMS, pop-up notification and/or emails to the roaming subscribers advising them to link their line with NIN or make effort to enroll for NIN if they do not have one within a specified time frame as may be determined by the NCC. - iv Communications Service Provider to share the MSISDNs of all outbound roamers with the NCC for the purpose of exempting such subscribers from the deadline issued by the Federal Government for NIN-SIM linkage. - v Nigerian citizen outbound roamers will be given a timeline of 18 months to visit Nigeria or a NIMC enrolment center in their Country of residence for the opportunity to enroll for a NIN.

B. EXISTING CORPORATE SUBSCRIBER - HARMONIZATION OF NIMC AND SIM REGISTRATION DATABASE

2.4. Corporate Demographic and Biometric Mismatch - Consent via USSD for NIN- SIM Registration

Update

Process flow	The below process flow shall apply: i. Subscriber provides Primary Telecom Master's Authorization Letter and NIN; ii. Communications Service Provider verifies Primary Telecom Master's NIN and confirms a mismatch or unavailability of Primary Telecom Master's SIM Registration;
---------------------	---

2.5. Corporate Subscriber Harmonization of NIMC and SIM Registration Database (Corporate & IOT/M2M)

1.	Context	This harmonization process shall apply the following scenarios: - i Where Primary Telecom Master biometrics (facial image) on the SIM Registration match with NIMC record but require demographic update; - ii Where Primary Telecom Master SIM Registration demographics match with NIMC record but require biometrics (fingerprint or facial Image) update; and - iii Where Primary Telecom Master SIM Registration demographics and biometrics do not match NIMC records and require a full update - iv Where Communications Service Provider has no record of existing corporate subscriber's Primary Telecom Master SIM Registration details. - v The above scenarios will require Consent from the Corporate as set out in Appendix 5. Consent can be via USSD, Email, SMS, Web Portal or Original Consent form filled physically.
----	----------------	---

		vi. Communications Service Provider calls up Primary Telecom Master's NIN records from NIMC database and eyeballs the said records vis-à-vis subscriber's passport photograph and verification form; vii. Where (iii) above is successfully completed, Communications Service Provider contacts subscriber to use deployed USSD code with options below: - a Press 1 to view your NIN records and adopt as SIM Registration KYC; - b Press 2 to visit COMMUNICATIONS SERVICE PROVIDER stores/centers to update SIM Registration KYC. viii. Where Option 1 is selected, Subscriber accesses Portal/Link where NIN records are displayed for subscriber to give consent; ix. NIN records and consent form shall be captured in one form for subscriber's approval; x. Subscriber reviews NIMC records and gives consent by filling necessary details and clicking the 'Accept' button; xi. OTP is triggered to Primary Telecom Master's MSISDN or official email address; xii. Communications Service Provider receives consent form and updates Primary Telecom Master's SIM Registration; xiii. Communications Service Provider sends SMS or email sent to Primary Telecom Master on successful SIM Registration update; xiv. Communications Service Provider stores all documents on subscriber's account.
--	--	--

2.6. Corporate Demographic and Biometric Mismatch - Consent via Physical Process for NIN- SIM Registration

Update

1.	Process flow	The below process flow shall apply: i. Corporate Subscriber represented by Primary Telecom Master, provides the Primary Telecom Master Authorization Letter and NIN; ii. Communications Service Provider verifies Primary Telecom Master's NIN and confirms a mismatch or unavailability of Primary Telecom Master's SIM Registration; iii. Communications Service Provider calls up Primary Telecom Master's NIN records from NIMC database, takes a Live Image and conducts electronic Facial Verification and case management which includes manual Facial Verification (eyeballing) on the Primary Telecom Master's passport photograph and Verification Form;
		iv. Where Facial Verification is successfully completed, Communications Service Provider notes the mismatch features and informs the Primary Telecom Master; v. Primary Telecom Master reviews' NIMC records and fills a physical Consent Form as approval to the Communications Service Provider to adopt the NIMC Foundational data as Functional data for the purpose of harmonization SIM Registration database for the Corporate Subscriber. vi. Communications Service Provider receives Consent Form and updates Primary Telecom Master's SIM Registration; vii. Communications Service Provider sends SMS or Email to Primary Telecom Master on successful SIM Registration update; viii. Communications Service Provider stores all documents on the corporate subscriber's account.

2.7. Subscriber Consent via SMS for SIM Registration KYC Update with NIN Records (Corporate & IOT/M2M)

1.	Process flow	The below process flow shall apply: i. Subscriber Provides Primary Telecom Master's Authorization Letter and NIN; ii. Communications Service Provider verifies Primary Telecom Master's NIN and confirms a mismatch or unavailability of Primary Telecom Master's SIM Registration; iii. Communications Service Provider calls up Primary Telecom Master's NIN records from NIMC database, takes a Live Image and conducts electronic Facial Verification and case-management which includes manual Facial Verification (eyeballing) on the Primary Telecom Master's passport photograph and Verification Form; iv. Where Facial Verification is successful, Communications Service Provider sends SMS to Subscriber with link to NIN records & Consent form. A sample of the Consent SMS request is set out in Appendix 6 to this Business Rules; v. Subscriber accesses Portal/Link where NIN records and Consent Form are displayed for subscriber consent and approval. vi. Subscriber review NIN records and gives consent by filling necessary details and clicking 'Accept' or 'Decline' button; OTP is sent to Primary TELECOM MASTER Line/official email address.
		vii. Where subscriber submits Consent Form, Communications Service Provider updates' SIM Registration with NIMC Foundational Data. viii. SMS or Email sent to Primary TELECOM MASTER on successful SIM Registration update. ix. All documents stored on the account

2.8 Subscriber Consent via COMMUNICATIONS SERVICE PROVIDER's Website for SIM Registration KYC Update with NIN Records (Corporate & IOT/M2M)

1.	Process flow	Subscriber Provides Primary Telecom Master's Authorization Letter and NIN; ii. Communications Service Provider verifies Primary Telecom Master's NIN and confirms a mismatch or unavailability of Primary Telecom Master's SIM Registration; iii. Communications Service Provider calls up Primary Telecom Master's NIN records from NIMC database and eyeballs the said records vis-à-vis subscriber's passport photograph and Verification Form; iv. Where (iii) above is successful, Communications Service Provider directs Primary Telecom Master to website hosting Consent Form; v. Subscriber accesses Portal/Link where NIN records are displayed for subscriber's consent; vi. NIN records and consent form are captured in one form for subscriber's approval; vii. Subscriber review NIN records and gives consent by filling necessary details and clicking 'Accept' or 'Decline' button; OTP is sent to Primary Telecom Masters' Line/official email address; viii. Where subscriber 'Accepts' Communications Service Provider receives Consent Form and updates SIM Registration; ix. SMS or Email sent to Primary Telecom Master on successful SIM Registration update; x. All documents stored on the account	
2	Website Requirements	i.	Communications Service Provider Website or Portal shall have available NIN records;
		ii.	In the case of mismatch, the mismatched details shall be displayed;
		iii.	Communications Service Provider Website or Portal shall display detailed Terms and Conditions of Acceptance;
		iv.	Subscriber shall have the option to accept or decline .

2.9 Subscriber Consent via Email for SIM Reg KYC Update with NIN Records (Corporate & IOT/M2M)

1	Process flow	i. Subscriber Provides Primary Telecom Master's Authorization Letter and NIN; ii. Communications Service Provider verifies Primary Telecom Master's NIN and confirms a mismatch or unavailability of Primary Telecom Master's SIM Registration; iii. Communications Service Provider calls up Primary Telecom Master's NIN records from NIMC database and eyeballs the said records vis-à-vis subscriber's passport photograph and Verification Form; iv. Where (iii) is successful, Communications Service Provider sends e-mail to the official e-mail address of the authorized Primary or Secondary Telecom Master containing a Scanned Form (containing NIN records & Consent provision) or link to Communications Service Provider Portal (containing NIN records & Consent Form); v. Where link is sent via email, Subscriber accesses Portal/Link where NIN records are displayed for subscriber's consent; vi. NIN records and Consent Form are captured in one form for subscriber's approval; vii. Subscriber reviews NIN records and gives consent by filling necessary details and clicking 'Accept' button; viii. OTP is sent to Primary Telecom Master's MSISDN/official email address; ix. Where subscriber 'Accepts', Communications Service Provider receives consent form and updates Telecom Master's SIM Registration KYC; x. Where Scanned Form is sent, Subscriber reviews NIN records and appends signature on Consent form; xi. Subscriber sends Consent Form back to Communications Service Provider (scanned and/or dispatched); xii. Communications Service Provider compares signature on other documents; xiii. Communications Service Provider updates SIM Registration with NIN records; xiv. Communications Service Provider notifies Telecom Master via Email upon successful SIM Registration KYC update; xv. All documents stored on subscriber's account.
---	---------------------	---

C. NEW SIM REGISTRATION/ACTIVATION CORPORATESFOR INDIVIDUALS, AND MACHINE-TO-MACHINE

The processes below should be read in conjunction with the Paragraph 1 – General Rules as it relates to the above subject matter.

NEW SIM REGISTRATION/ACTIVATIONS FOR INDIVIDUALS

2.10 Subscriber Acquisition (SIM Sales) Process

	This flow covers below scenarios. a) Where new Subscribers with NIN requests new SIM; b) Where existing Subscribers with NIN requests additional SIMs; c) Where new or existing Foreign Subscriber requests SIM acquisition/activation d) Where new or existing Diplomatic Missions/Embassies request SIM acquisition/Mobile Network Portability (MNP) e) Where a Subscriber with NIN requests MNP service; f) Where a new or existing subscriber without NIN requests a new SIM or MNP service; g) Where Communications Service Provider seeks to re-cycle MSISDNs with NIN.
--	---

2.11 New Subscriber Acquisition with NIN (SIM Sales)

	This flow covers below scenarios. a) Where a new Subscriber with NIN requests SIM Acquisition/Activation; b) Where new Subscribers' NIN and facial matches data on NIMC database.
--	--

2.12 New SIM Acquisition/SIM Sales Business Guidelines

2.1	Activation Scenario	New Subscriber with NIN requesting SIM acquisition/activation and the Subscribers' NIN and biometric (i.e. Fingerprint or Facial Image) is the same with NIMC.
-----	----------------------------	--

	Process Flow	Subscriber requests new SIM activation; i. Communications Service Provider verifies NIN from NIMC database;
--	---------------------	---

		ii.	Where a P1 service outage is occasioned during NIN verification, Communications Service Provider should refer to Appendix 3 Service Level Requirement with NIMC and Limited Service Offerings to Subscribers.
		iii.	Communications Service Provider to capture Biometrics (in this case Facial live image or Fingerprints) and send Facial Image to the backend for electronic facial verification and case management which includes manual Facial Verification (eyeballing).
		iv.	Where Subscriber's NIN and biometric (i.e. Facial image or Fingerprint) matches with records from NIMC database, Communications Service Provider obtains Subscriber consent and copies NIMC Foundational data which becomes Communications Service Provider Functional Data for the purpose of SIM registration;
		v.	Communications Service Provider completes SIM Registration with captured Live Image;
		vi.	Communications Service Provider issues MSISDN to subscriber;
		vii.	Communications Service Provider activates subscriber's MSISDN and saves subscriber's Sim Registration information.

2.13 Existing Subscriber with NIN		
		This flow covers below scenarios: - a Where existing Subscriber with NIN requests new SIM activation; - b Where existing subscriber's NIN and Fingerprint or Facial Image matches the biometrics on both NIMC and existing SIM Registration database.
1.	Activation Scenario	Existing Subscriber's NIN and Facial Image matches the biometrics on the NIMC database.

2.	Process Flow	i. Subscriber requests new SIM activation; ii. Communications Service Provider verifies NIN from NIMC database; iii. Communications Service Provider to capture biometrics (Facial Live Image) and sends the Facial Image to the backend for electronic Facial Verification and case management which includes manual Facial Verification (Eye-balling). iv. Where a P1 service outage is occasioned during NIN verification, Communications Service Provider should refer to Appendix 3 Service Level Requirement with NIMC and Limited Service Offerings to Subscribers;
		v. Communications Service Provider shall obtain Consent, copy and update Subscriber's SIM Registration with NIMC Foundational details where there is a mismatch; vi. Where the Subscriber is requesting for additional SIM for the first time and NIN SIM harmonization is required, Communications Service Provider will copy and duplicate NIMC Foundational details unto SIM Registration database; vii. Where NIN-SIM harmonization has been performed, Communications Service Provider duplicates and copies SIM Registration to subscriber's new MSISDN; viii. Communications Service Provider activates subscriber's MSISDN and saves subscriber's Sim Registration information.

2.14 New and Existing Subscriber (Foreigners) SIM Acquisition/Activations

	□ This process should be read and applied in line with the General Rules on Foreigners SIM Activation as set out in Paragraph 1 – General Rules.
	This flow cover below scenarios; a. Foreigners with Legal Residency status or two (2) years and above. b. Foreigners with visitors' visas (with visas less than two (2) years). c. Foreigners transiting through Nigeria or employed or reside in Nigeria for less than two (2) years. d. Foreigner with Diplomatic visas (including family diplomatic visa)

1.	Activation Scenario	Foreigners with Legal Residence Status of two (2) years and above - Refers to the process on New SIM Activation (including MNP) for New and Existing Subscribers - NIN is mandatory - Where Foreigners are without NIN, Communications Service Providers can capture and enroll the resident for NIN issuance upon presentation of Residents Permit Foreigners with Visitors Visas (with Visas less than two (2) years) - NIN is not mandatory or required - Upon request to purchase a New SIM or additional SIM, Communications Service Provider will request and capture the following on their records as proof of identity of the Foreign Subscriber - International Passport Bio-Data page and - Visa page The following process will be applicable for the purpose of New SIM activations and Additional SIM activations; - The Foreigner presents a Visa and Communications Service Provider collects copy of same. - The Foreigner in addition to the above presents the International passport page that contains the NIS Immigration entry stamp and Communications Service Provider collects same as corroboration of NIS validation.
----	---------------------	---

		• Communications Service Provider should verify to confirm that the date on the NIS entry stamp falls within the visa start and end dates. • Communications Service Provider captures the International passport page and number. • Communications Service Provider captures the walk-in image and NIN based demographic details of the Foreigner. The Foreigner's name that is captured should match with the name on the visa. • Communications Service Provider will perform electronic facial verification and case-management which includes manual facial verification, (eyeballing) of the live Image with visa page picture for matching. • Communications Service Provider will configure the activation period of the new SIM to 6 months. • Communications Service Provider issues SIM to Foreigner and activates same. • SIM is automatically deactivated at 6 months. SIM can be reactivated for another 6 months were the visa validity period is more than 6 months but does not exceed 2 years and the Foreigner has made a request for such a renewal. • Communications Service Providers are to collate the International Passport Number to send to NIS for validation on a weekly basis. • Where NIS returns the details of the International Passport Number as invalid then the line will be deactivated. • This process will apply to New SIM Activations (including MNP) for New and Existing Subscriber. • All other processes in the New SIM Activation for New and Existing Subscriber is applicable save for the requirement of NIN validation and verification.
		Foreigners transiting through Nigeria or are employed in or reside in Nigeria for less than 2 years ☐ NIN is not mandatory and required

		• Upon the request to purchase a New SIM or additional SIM or MNP, Communications Service Provider will request and capture the following on their records as proof of identity of the Foreign subscriber; • International passport bio-data page and • Visa page • The following process will be applicable for the purpose of New SIM activations and Additional SIM activations: • The Foreigner presents a Visa and Communications Service Provider collects copy of same. • The Foreigner in addition to the above presents the International passport page that contains the NIS Immigration entry stamp and Communications Service Provider collects same as corroboration of NIS validation.
--	--	--

		• Communications Service Provider should verify to confirm that the date on the NIS entry stamp falls within the visa start and end dates. • Communications Service Provider captures the International passport page and number. • Communications Service Provider captures the Live image, and NIN based demographic details of the Foreigner. The Foreigner's name that is captured should match with the name on the visa. • Communications Service Provider will perform electronic facial verification and case-management which includes manual facial verification (eyeballing) of the live Image with visa page picture for matching. • Communications Service Provider will configure the activation period of the New SIM for a period of 2 weeks/1 month/3 months as applicable to the Visa validity and can be renewed further upon request and where the visa is not for a stay of 2 years and above. • Communications Service Provider issues SIM to Foreigner and activates same. • SIM is automatically deactivated at 2 weeks/1 month/3 months as applicable to the Visa validity. SIM can be reactivated for another 3 months where the visa validity period is more than 6 months but does not exceed 2 years and the Foreigner has made a request for such a renewal.
--	--	--

		• Communications Service Providers are to collate the International Passport Number to send to NIS for validation on a weekly basis. • Where NIS returns the details of the International Passport Number as invalid then the line will be deactivated. • This process will apply to New SIM Activations (including MNP) for New and Existing Subscribers. • All other processes in the New SIM Activation for New and Existing Subscriber is applicable save for the requirement of NIN validation and verification. Foreigners with Diplomatic visas (including family diplomatic visa) staying for 2 years or more • Refer to the process on New SIM Activation for New and Existing Subscriber. • NIN is mandatory. • Where Foreigners are without NIN, Communications Service Provider can capture and enroll the Resident for NIN issuance upon presentation of residents' permit • Where the Foreigner with Diplomatic visa is staying for less than 2 years the following documents will be retrieved by the
--	--	--

		Communications Service Provider in the course of a new SIM sale/activation process for record keeping: ☐ International passport biodata and; ☐ Letter from the Embassy that their stay is for less than 2 years
--	--	---

2.15 Subscriber Acquisition and SIM Sales Process (Corporate & IoT/M2M Subscribers)

New SIM Registration/ Activation are grouped into 3 Scenarios-

1. New Subscriber with NIN requesting New SIM
2. Existing Subscribers with NIN requesting for additional SIM
3. Subscribers (New and Existing) requesting New SIM or Porting without NIN

2.16 New SIM Registration/Activation Business Guidelines (Corporate & IOT/M2M)

2.17 New Subscribers with NIN (Corporate and IOT/M2M)

This flow covers below scenarios

New Corporate Subscriber with Primary Telecoms Master NIN requesting SIM Acquisition (Physical visit for SIM Registration)

1.	Scenario	New Corporate Subscriber with Primary Telecoms Master NIN requesting SIM Acquisition (Physical visit for SIM Registration is required).
----	-----------------	---

2.	Process Flow	1. Corporate Subscriber (via the Primary TELECOM MASTER) approach Communications Service Provider for SIM Acquisition/ New SIM 2. Corporate Subscriber provides Request letter & other mandatory requirements (CAC Registration Number and CAC Incorporation document, TIN, order Forms, Utility Bills, etc. 3. Communication Service Providers confirms complete documentation & issues range of SIMs to corporate Subscribers i.e. SIM Serials and MSISDNs. 4. Corporate Subscriber selects on SIM (MSISDN) for authorized Primary Telecom Master & notifies Communications Service Provider; 5. Subscriber provides TELECOM MASTER Authorization letter, signed Indemnity Form and List of lines, proposed users First Name and Last Name, their NINs & alternative phone numbers (List not applicable for IOT/M2M) 6. Communications Service Provider calls NIMC database API to verify Primary Telecom Master's NIN and biometrics (i.e. Facial image). Primary Telecom Master's Line is fully activated, if NIN is successfully validated and verified; 7. In the case of Facial Verification, Communications Service Provider captures Live image of Primary Telecom Master and executes electronic Facial verification and case-management which includes manual facial verification (eye-balling). 8. Where Primary Telecom Master's NIN and biometric (facial image) matches with records from NIMC database, Communications Service Provider collects Primary Telecom Master's consent and copies NIMC Foundational data which becomes Communications Service Provider's functional data for the purpose of SIM registration; 9. Communications Service Provider uses live image of the Primary Telecom Master as biometrics for SIM Registration process. 10. Communications Service Provider must ensure Secondary NINs are validated. Associated Secondary lines are fully activated if secondary NINs are successfully validated (Not Applicable for IOT/M2M) 11. Where Secondary NIN validation fails the lines will not be activated.
----	---------------------	---

		12. Once NIN is used to activate corporate lines, an SMS will be sent to the provided alternative mobile phone numbers notifying the Users of the corporate lines that their NINs have been linked to the corporate account of their Employer. 13. Where a P1 service outage occurs during verification of Primary Telecom Master and validation of Secondary NIN, Communications Service Provider should refer to the work around set out in Appendix 3 Service Level Requirement with NIMC and Limited Service Offerings to Subscribers.
--	--	---

2.17 Existing Subscribers With NIN (Corporate & IOT/M2M)

This flow covers below scenarios.

1. Existing Corporate or IOT/M2M subscriber with Primary TELECOM MASTER NIN requesting additional SIM (which includes subscription medium) 2. Primary TELECOM MASTER SIM Registration mismatch with NIN details or Primary TELECOM MASTER SIM Registration not available		
1.	Process Flow	1. The Primary or Secondary Telecom Master approach Communications Service Provider, for additional SIM (which includes subscription medium) this can be done via Emails, Request letter or Sales orders. 2. Communications Service Provider confirms full compliance with new Corporate Telecom Master rules.

		3. Communications Service Provider confirms Primary NIN validation/verification status and Secondary NIN validation status (not applicable for IOT/M2M). 4. In the case of facial verification, Communications Service Provider will effectively verify the Primary Telecom Master's NIN data and match with SIM Registration using electronic Facial verification and case-management which includes manual facial verification (eye-balling); 5. Where Corporate Telecom Master rules is irregular, Secondary Telecom Master regularizes Corporate account (i.e submits TELECOM MASTER authorization Letter, duly executed Indemnity forms, and all other relevant documents as set out in the Paragraph 1 - General Rules etc). 6. Where there is Primary TELECOM MASTER NIN/SIM Registration database mismatch or new Primary TELECOM MASTER SIM Registration is not available (Communications Service Provider to refer to Existing Corporate Subscriber – Harmonization of NIMC-SIM Registration database). 7. Primary or Secondary Telecom Master provides duly filled Verification Form: Primary TELECOM MASTER details with Passport Photograph & Consent to use NIN data. 8. Communications Service Provider executes electronic facial verification and case management which includes manual facial verification (eye-balling) process to treat mismatch & verify Primary TELECOM MASTER NIN. 9. Where Number8 is successful, copy & update Primary TELECOM MASTER SIM Registration with NIMC Foundational detail. 10. Subscriber provides list of users of new lines with Secondary NIN and Names and Alternative Phone Numbers (not applicable for IOT/M2M). 11. Validate Secondary NIN and link to additional SIMs; upload list of additional Secondary NIN 12. Where a P1 service outage occurs during verification of Primary Telecom Master and validation of Secondary NIN, Communications Service Provider should refer to the work around set out in Appendix 3 Service Level Requirement with NIMC and Limited Service Offerings to Subscribers. 13. Link Primary TELECOM MASTER SIM Registration and NIN on all new additional SIMs 14. Send SMS to alternate phone numbers provided in list of additional lines notifying the Users of the Additional lines that their NINs have been linked to the Corporate account of their Employer. 15. Activate additional SIM/MSISDN & Save.
--	--	---

2.18 DIPLOMATIC MISSIONS AND EMBASSIES

This flow covers below scenarios.

A. Diplomatic Mission (New or Existing Subscriber) requesting SIM Acquisition or MNP

1.	Activation Scenario	(New & existing) Diplomatic Mission or Embassy subscriber requesting New SIM or Porting with NIN
2.	Process Flow	i. In respect of an Embassy and Diplomatic Mission requesting for SIM Acquisition or MNP the following process shall apply: a) The Head of Mission will approach the Communications Service Provider to request for SIMs (which includes subscription medium) by providing to the Communications Service Provider the following; b) The data page containing the passport number of the diplomatic passport of the Head of Mission/Embassy along with a Letter of Request signed by the Ambassador or its equivalent for registration of the official telephone lines of the Embassy/Mission in Nigeria shall be submitted to the Ministry of Foreign Affairs for verification and confirmation and registration of the SIMs; c) For the registration of SIM (which includes subscription medium) of Diplomatic Missions, the following are required: i. The Data page containing the passport number of the Diplomatic Passport of the Head of Mission/Embassy. ii. A Letter of Request signed by the Ambassador or its equivalent. iii. Letter verifying and confirming registration of SIMs by the Ministry of Foreign Affairs. ii. Any Foreign member of a diplomatic mission requiring SIMs for personal use shall go through the processes under item 8 respect of Foreigners with Visas less than 2 years;

PART III. MOBILE NUMBER PORTABILITY (MNP) INDIVIDUALS AND CORPORATE SUBSCRIBERS

The MNP Regulations and MNP Business Rules and Processes 2014 is the governing instrument to ensure an effective and efficient porting regime in the Communication industry. Given the fact that the introduction and mandatory use of NIN has become a pre-requisite feature in all Communications service transactions, it is imperative to adapt the MNP rules to give force to the Revised National Identity Policy for SIM Card Registration. The following processes shall be read and applied in conjunction with the existing MNP Regulations and Business Rules and Processes (2014).

3.0 Individual Subscribers with NIN requesting Mobil Number Porting (MNP)

This flow covers below Scenarios

- A. Subscriber with NIN requesting Mobile Number Porting (MNP)
- B. Subscriber NIN, Fingerprint or Facial Image is the same with NIMC

1.	Activation Scenario	Subscribers NIN and Facial Image is the same with NIN	
2.	Process Flow	i.	Subscriber approach Communications Service Provider for MNP
		ii.	Communications Service Provider calls NIMC API to verify Subscribers' NIN and Biometric (including Fingerprint and Facial Image)
		iii.	In the case facial verification, Communication Service Provider will effectively verify the subscribers' NIN data and using electronic Facial verification and case management which includes manual facial verification (eye balling)
		iv.	In the case of a Foreigner, the General Rules on Foreigner SIM acquisition/activation with respect to proof of identity will be applicable for verification purpose.
		v.	In the case of Diplomatic Mission and Embassies, the General Rules on Diplomatic Missions and Embassies SIM acquisition/activation with respect to proof of identity will apply for verification purposes.
		vi.	Where verification is successful, Communications Service Provider is to collect subscriber consent to copy NIMC Foundational Data as Financial Data for SIM Registration
		vii.	Complete SIM Registration with Live Image.
		viii.	Activate MNP Service & Save

		ix. All other MNP Business Rules remain valid and in force.
--	--	---

3.1 New Subscribers with NIN requesting Mobile Number Portability (MNP) Corporate & IOT/M2M

This flow covers below Scenarios

- A. New Subscriber with NIN requesting Mobile Number Porting (MNP)
- B. Subscriber demographics, biometrics and NIN match with NIMC database

1.	Scenario	1. New Subscriber with NIN requesting Mobile Number Porting (MNP) 2. Subscriber demographics, biometrics and NIN match with NIMC database
2.	Process Flow	1. Corporate Subscriber approaches Communications Service Provider for Mobile Number Portability (MNP); 2. Primary Telecom Master provides TELECOM MASTERS Authorization (with Primary TELECOM MASTER NIN), Indemnity form, Last Invoice & List of Secondary Users and NIN (not applicable for IOT/M2M); 3. Communications Subscriber Provider verifies Primary TELECOM MASTER NIN with NIMC database, if unsuccessful, reject MNP; 4. In the case of facial verification Communications Service Provider will effectively verify the Primary Telecom Masters NIN data using electronic Facial verification and case-management which includes, manual facial verification (eye balling); 5. Communications Service Provider captures live image of the Primary Telecoms Master, collects Primary Telecom Master using NIMC Foundational Data. 6. Communications Service Provider validates secondary NIN records with NIMC Foundational Data (Not applicable for IOT/M2M) If unsuccessful, reject MNP;
		7. Communications Service Provider to link Primary Telecom Master SIM Registration and NIN on all New SIMs;
		8. Link Secondary NIN to each SIM on the system;
		9. Activate Service & Save; 10. Upload the list of Secondary Users NIN, First Name, Middle Name, Last Name and Alternative phone numbers; 11. Send SMS to alternate phone numbers provided in list of additional lines; 12. Actively newly ported SIMs/MSISDN and Save.

		13. All other MNP rules remain valid.
--	--	---------------------------------------

3.2. Existing Subscribers With NIN requesting Mobile Number Porting (MNP) (Corporate & IOT/M2M)

This flow covers below scenarios.

1. Existing Subscriber with NIN requesting Mobile Number Porting (MNP)

requests to port its Corporate SIMs from its corporate accounts with Communications Service Provider (B) to its corporate account held with Communications Service Provider (A) or vice versa.

3. Primary TELECOM MASTER SIM Registration mismatch with NIN details or Primary TELECOM MASTER SIM Registration not available

	Scenario	- Existing Subscriber with NIN requesting Mobile Number Porting (MNP) - Where an Existing Subscriber has some Corporate SIMs with a particular Communications Service Provider (A) and others in another Communications Service Provider (B) and requests to port its Corporate SIMs from its corporate accounts with Communications Service Provider (B) to its corporate account held with Communications Service Provider (A) or vice versa. - Primary TELECOM MASTER SIM Registration mismatch with NIN details or Primary TELECOM MASTER SIM Registration not available.
	Process Flow	- Primary or Secondary Telecom Master approach Communications Service Provider for MNP; - Subscriber provides Telecom Master Authorization, Indemnity form, Last Invoice & List of Secondary users, Primary Telecom Master's NIN etc. (not applicable for IOT/M2M); - Communications Service Provider verifies Primary Telecom Master NIN against NIMC database;

		4. Where there is Primary TELECOM MASTER NIN/SIM Registration mismatch or new Primary TELECOM MASTER SIM Registration is not available, refer to Existing Corporate Subscriber – Harmonization NIMC-SIM process; 5. Subscriber provides Verification Form: Primary TELECOM MASTER details with Passport Photograph & Consent Form to use NIMC Foundational data as Functional data for SIM Registration.
		6. Communications Service Provider executes electronic Facial Verification and Case-management which includes manual Facial verification (eye-balling) process to treat mismatch & effectively verify Primary TELECOM MASTER NIN;
		7. Where verification is successful, copy & update Primary TELECOM MASTER SIM Registration with NIMC Foundational details;
		8. Subscriber provides list of Secondary users with Secondary NIN and Names and Alternative Phone Numbers (not applicable for IOT/M2M); 9. Validate Secondary NIN and link to SIMs; upload list of Secondary users, NIN and other relevant Corporate Account documents; 10. Link Primary TELECOM MASTER SIM Registration and NIN on all SIMs; 11. Send SMS to alternate phone numbers provided in list of Secondary users 12. Activate additional SIMs/MSISDN and Save.
2. Where an Existing Subscriber has some Corporate SIMs with a particular Communications Service Provider (A) and others in another Communications Service Provider (B) and		

PART IV: CHURN AND RECYCLING OF SUBSCRIBER SIM ACTIVATION

The Quality of Service Regulations 2024 stipulates the procedure for the treatment of a Subscriber/Subscriber's Lifecycle on the Communications network of the Communications Service Provider. Given the fact that the introduction and mandatory Use of NIN has become a pre-requisite feature in all Communications service transactions, it is imperative to adapt the provisions of the Quality of Service Regulations 2024 – as it relates to Subscriber Lifecycle to give force to the Revised National Identity Policy for SIM Card Registration.

The following processes shall be implemented in conjunction with the Quality of Service Regulations (2024) with respect to compliance with the provisions on Subscriber's/Subscriber lifecycle (Recycling and churn of Subscribers SIM activations).

4.0. Churned and Recycled SIM Activation

This flow covers below scenarios.

1. Recycling MSISDN with NIN
2. Where MSISDN of subscribers with NIN is inactive for a period of 360 days and has fallen due for Recycling based on the QoS Regulations 2013.

1.	Activation Scenario	Recycling for subscribers with submitted /linked NIN
2.	Process Flow	i. Communications Service Provider to Purge NIN from Recycled MSISDN. ii. Call Recycle API to NCC Central Database, NIMC & NIBSS for Financial Institutions. iii. Communications Service Provider Keep SIM Registration &NIN History for 2 years
3.	Points to Note	All recycled SIMs shall be purged of any NIN attached, this is to allow New subscriber submit and link NIN

4.1. Churned and Recycled SIM Activation for Foreigners

This flow covers below scenarios.

1. Recycling MSISDN with NIN
2. Where Foreigner subscribers with NIN is inactive for a period of 360 days and due for Recycling
3. Foreigners with Visitors Visa with visas less than 2 years
4. Foreigners transiting through Nigeria or legally resident in Nigeria for less than 2 years.
5. Diplomats with stay less than 2 years

1.	Activation Scenario	1. Recycling MSISDN with NIN 2. Where Foreigner subscribers with NIN is inactive for a period of 360 days and due for Recycling 3. Foreigners with Visitors Visa with visas less than 2 years 4. Foreigners transiting through Nigeria or legally resident in Nigeria for less than 2 years. 5. Diplomats with stay less than 2 years
2.	Process Flow	i. A Foreigner with a Nigerian visa with visa period less than two (2) years is required to present his/her international passport and visa page to the Communications Service Provider prior to activation of a SIM for local Communications service. ii. In activating the SIM, the Rules on New Acquisition/Sales to Foreigners will be applicable. iii. Where a Foreigner has the intention of returning to Nigeria after the expiration of visa period within a maximum two (2) year period, and is desirous of retaining the line beyond the Visa period due to personal or business reasons, such Foreigner is required to make an application to the Communications Service Provider requesting for a 'Keep My Line' service via any channel of official communication provided by the Communications Service Provider. iv. A copy of the Foreigner's valid passport and visa page should accompany the application.
		v. Further to review of the subscriber's application, the Communications Service Provider may extend the activation period for additional 90days period in the first instance. Subsequent extension request(s) which must be based on a request by the Foreigner, shall not exceed a maximum period of two (2) years (which includes the initial Visa period).

		vi. Where a Foreigner fails to make a request for the keep my line service or extension or where such request is declined by the Communications Service Provider with reasons provided to the foreigner, such line shall be deactivated and recycled by the Communications Service Provider in compliance with the Quality of Service Regulations (2013). vii. Where a Foreigner has retained a line for the maximum period of 2 years period cumulatively, such a Foreigner will be advised to secure a NIN. For the avoidance of doubt, this process (activation of lines for foreigners) does not apply to Nigerian citizens who are eligible for a NIN.
3.	Points to Note	All recycled SIMs shall be purged of any NIN attached, this is to allow New subscriber submit and link NIN

4.2. Recycling (Corporate & IOT/M2M)

This flow covers below scenarios.

1. Recycling corporate MSISDN with NIN
2. Where subscribers with NIN is inactive for the period of 360 days and due for Recycling

1.	Process Flow	• Communications Service Provider to purge both Primary & Secondary NIN from Recycled MSISDN • Communications Service Provider to call Recycle API to NCC Central Database, NIMC & NIBSS for Financial Institutions • Communications Service Provider keep Primary TELECOM MASTER SIM Registration & Secondary NIN History for that particular line in an archive for 2 years (from date of recycle) Recycling policies for corporate subscribers apply
2.	Points to Note	All recycled corporate and IOT/M2M SIMs shall be purged of any NIN attached, this is to allow New subscriber submit and link their NIN

4.3 Policy on Inactive Account Management and Churn

This policy establishes guidelines for managing customer registrations that remain inactive beyond a defined revenue-generating period, ensuring alignment with operational efficiency and regulatory compliance.

1.	Inactivity Threshold	Accounts failing to trigger an RGE within 365 consecutive days shall be classified as Inactive and subject to delinking of NIN and churning of the line.
2.	Delinking & Churn Process	• All inactive accounts shall be delinked from operational systems of NIMC (NIN delinking). • Services associated with such accounts shall be churned (terminated). • Number is returned to pre-registration state.

ART V: PROCESS FLOW FOR NON-GSM, PNLs & ISPs

5.1.PHYSICAL: NEW CUSTOMER (CORPORATE) SEEKING TO PURCHASE NON-GSM/PNL/ISP SERVICES

- Start
- Customer requests for Non-GSM/PNL/ISP Service purchase & activation
- Sales Manager informs customer of requirements for activation with relevant templates via email
- As a new customer, Primary Telecoms Master is required to come into a Non-GSM/PNL/ISP owned shop for Bio Data capture.
- Primary TM is registered with the Service Pilot Number
- Primary TM provides all documentation required – listed
- Primary TM provides all services listed per Trunk/location/capacity/DID-DOD in a CSV file
- Non-GSM/PNL/ISP validates customer documentation against already submitted documentation to ensure full alignment
- Non-GSM/PNL/ISP also conducts a physical validation of customer's operational HQ and the location where the service is being used. Service request is denied if this is not concluded positively.
 - Non-GSM/PNL/ISP sends Primary TM VNIN to NIMC for verification
- Non-GSM/PNL/ISP Copy NIMC foundational details returned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID)
- Non-GSM/PNL/ISP compares image from submitted documentation – Customer ID + Customer image retrieved from NIMC.
- Non-GSM/PNL/ISP approves or reject KYC based on Images compared.
- If approved customer information is saved
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals. Customer details below,
- Service is activated within 24hrs of NCC notification
- End

5.2 PHYSICAL: CALL CENTER LICENSEE SEEKING TO PURCHASE NON-GSM /PNL SERVICES

- Start
- Customer requests for Non-GSM/PNL/ISP Service purchase & activation
- Sales Manager informs customer of requirements for activation with relevant templates via email
- As a new customer, Primary Telecoms Master is required to come into an Non-GSM/PNL/ISP owned shop for bio data capture
- Primary TM is registered with the Service Pilot Number
- Primary TM provides all documentation required – listed (Including NCC License)
- Primary TM provides all services listed per Trunk/location/capacity/DID-DOD in a CSV file
- Non-GSM/PNL/ISP validates customer documentation against already submitted documentation to ensure full alignment
- Non-GSM/PNL/ISP sends Primary TM VNIN to NIMC for verification
- Non-GSM/PNL/ISP Copy NIMC Foundational Details retuned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID)
- Non-GSM/PNL/ISP compares image from submitted documentation – customer ID + Customer image retrieved from NIMC.
- Non-GSM/PNL/ISP approves or reject KYC based on Images compared.
- If approved customer information is saved
- Non-GSM/PNL/ISP also conducts a physical validation of customer's operational HQ and the location where the service is being used. Service request is denied if this is not concluded positively
- MNO/PNL creates VAS-CCS Profile on Web-portal for onboarding their 3rd Party Customers.
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals. Customer details below,
- Service is activated within 24hrs of NCC notification
- End

5.3 PHYSICAL. NEW CUSTOMER (INDIVIDUAL) SEEKING TO PURCHASE PNL/ISP SERVICES

- Start
- Customer approaches PNL/ISP for Service purchase & activation.
- Customer submits NIN to PNL/ISP
- PNL/ISP Verify NIN via Aggregator Service (basic verification) - Customer NIN+ Biometric (FP/Facial Image/Iris) is the same with NIMC
- Where Subscriber information matches with NIMC, MNOs copy NIMC Foundational Details (Demographic & Image)
- Complete KYC and take live image of the Subscriber
- Capture Biometrics (Live Image) in accordance with the standards in Appendix 8 of these Business Rules and as determined by the NCC over time.
- PNL/ISP issue CPE to Customer
- Activate & Save
- End

5.4 ONLINE NEW CUSTOMER (INDIVIDUAL) SEEKING TO PURCHASE PNL/ISP SERVICES

- Start
- Customer visits PNL/ISP Online Website for purchase & activation.
- PNL/ISP Website provides customer with KYC requirements.
- Customer fills & attach all KYC documentation required online (including NIN & Location)
- Location verified by PNL/ISP (FTTH-SAT-FW)
- Customer is Re-directed to Verification Portal
- Customer's image is captured on Verification Portal
- Send Customer VNIN to NIMC for verification
- Copy NIMC foundational details returned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID)
- Compare image from submitted documentation – customer ID + Customer image retrieved from NIMC.
- Approve or reject KYC based on Images compared.
- If approved, sends Customer information to PNL/ISP to save.
- Customer receives confirmation via PNL/ISP Web Portal, Email & Alternate Number
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals.
- Service is activated within 24hrs of NCC notification
- End

5.5 ONLINE NEW CUSTOMER (CORPORATE) SEEKING TO PURCHASE NON-GSM /PNL/ISP SERVICES

- Start
- Customer visits MNO/PNL/ISP Online Website for purchase & activation.
- MNO/PNL/ISP Website provides customer with KYC requirements.
- Customer fills & attach all KYC documentation required online (including TM NIN & Location)
- Location verified by MNO/PNL/ISP (FTTH-SAT-FW)
- Customer is Re-directed to Verification Portal
- Customer's TM image is captured on Verification Portal
- Sends Customer TM VNIN to NIMC for verification
- Compares image from submitted documentation – customer ID + Customer TM image retrieved from NIMC.
- Approve or reject KYC based on Images compared
- If approved, Copy NIMC foundational details returned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID) else terminate process
- If approved, save Customer information.
- MNO/PNL/ISP creates Profile on Web-portal for onboarding their Corporate Customers (OTP required from TM per request)
- Customer receives confirmation via MNO/PNL/ISP Web Portal, Email & TM number
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals.
- Service is activated within 24hrs of NCC notification
- End

5.6 ONLINE CALL CENTER LICENSEE SEEKING TO PURCHASE NON-GSM /PNL SERVICES

- Start
- Customer visits MNO/PNL Online Website for purchase & activation.
- MNO/PNL Website provides customer with KYC requirements.
- Customer fills & attach all KYC documentation required online (including NCC License, NIN & Location)
- NCC License & Location verified by MNO/PNL
- Customer is Re-directed to Verification Portal
- Customer's image is captured on Verification Portal
- Send Customer VNIN to NIMC for verification
- Compare image from submitted documentation – customer ID + Customer image retrieved from NIMC.
- Approve or reject KYC based on Images compared.
- If approved, Copy NIMC foundational details returned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID)
- If approved, save Customer information
- MNO/PNL creates VAS-CCS Profile on Web-portal for onboarding their 3rd Party Customers

- Customer receives confirmation via MNO/PNL Web Portal, Email & TM number.
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals.
- Service activation dependent on 3rd party Validation.
- End

5.7 ONLINE KYC 3RD PARTY ONBOARDING PROCESS FOR CALL CENTER LICENSEES

- Start
- Customer visits VAS-CCS Online Website to request for service (Numbering range).
- VAS-CCS goes to its Profile on MNO/PNL Online Web Portal & allocates Number range to Customer
- VAS-CCS request Customer to provide KYC requirements via MNO/PNL Online Web Portal (integration required to MNO/PNL Portal)
- Customer fills & attach all KYC documentation required online (including TM-2 NIN & Location)
- Customer is Re-directed to Verification Portal
- TM-2's image is captured on Verification Portal
- Send TM-2 VNIN to NIMC for verification
- Compares image from submitted documentation – Customer ID + TM-2 image retrieved from NIMC.
- Approve or Reject KYC based images compared.
- If approved, copy NIMC Foundational details returned from NIMC (Ref Level 4: Payload- i.e. - Image, First name, Last name, Gender, DOB, User ID)
- If approved, MNO/PNL Save TM-2 information & notifies VAS-CCS.
- TM-2 receives confirmation via MNO/PNL Web Portal, E-mail & number.
- Customer information is shared to the NCC informing of service being requested for and KYCNIN approvals.
- Service (Number range) is activated within 24hrs of NCC notification.
- End

5.8 RULES FOR NON-GSM/ISP/PNL ONLINE KYC

- 1) All Non-GSM/ISP/PNL will be carried out via physical or online channels;
- 2) There will be a single online KYC verification portal available for ISPs/PNLs;
- 3) VAS CCS Licensee will be required to provide details of 3rd Party Company requesting for Call Center Services (via MNO/PNL's Online Portal);
- 4) Call Centers process will have 2 Telecoms Masters (TM1=VAS-CCS, TM2= 3rd Party Company);
- 5) Fixed locations "PNL/ISP (Fixed Wireless, Satellite, FTTH)" will require location verification;
- 6) Service Providers with more than 60,000 Subscribers may deploy their online KYC Service (In Line With Approved Specifications);
- 7) MNOs/Major ISPs may opt to use online KYC Aggregator Service;
- 8) Online KYC Aggregator Service should be adopted for MVNO providers;

All Corporate Telecom Master must sign an Indemnity Form & is Responsible for any fraud carried out by its Number Range.

5.9 KYC DOCUMENTS REQUIREMENTS

- 1) National Identification Number (NIN).
- 2) Authorization Letter;
- 3) Indemnity Letter;
- 4) Consent Form;
- 5) All services listed in a CSV document;
- 6) Certificate of Incorporation OR Public/Government organizations are to present Legal Instrument showing evidence of establishment;
- 7) Location/Address;
- 8) Tax Clearance Certificate/TIN;
- 9) Passport Picture of Primary Telecoms Master; 10) All payment evidences.

PART VI: GOVERNANCE

6.1 Governance for Agents and Device handlers

The objective of this governance rule is to ensure that the SIM Registration Agents/Dealers and Device Handlers do not pose avoidable threat to the sanity of data that NIN, SIM registration and integration process intends to address.

		1. All Dealers and Device handlers engaged by Communications Service Providers for SIM Registration are to be licensed by the NCC and accredited by the MNO's and their details forwarded to the NCC; 2. Details of all enrolment devices and sims assigned to each dealer are to be forwarded to the NCC; 3. The NCC will liaise with security agents to undertake security checks on all dealers and agents. Any agent/dealer with adverse security report will not be engaged and blacklisted as the case may be 4. Communications Service Providers are to accredit enrolment agents engaged by their dealers and forward details of all engaged agents to the commission 5. Enrolment agents must possess a NIN and BVN, details of which are to be forwarded to the NCC; 6. Enrolment agents must have minimum educational qualification of Secondary School Certificate (SSCE/WAEC); 7. Communications Service Providers shall not make cash payments to enrolment agents as commission or incentive. All payments are to be made through agent's bank accounts; 8. Communications Service Provider should put in place mechanisms to ensure that front-end SIM Registration and NIN verification systems have a timeout period to restrict the ability of Registration Agents as well as Geo fencing the devices assigned to them.
--	--	--

		9. Communications Service Provider to provide details of dealers/agents that registered SIM
--	--	---

		(which includes subscription medium) that have been identified as fraudulently registered 10. Communications Service Provider to have a mechanism for flagging off suspected infractions in sim registration and the SIMs involved in such infractions should be deactivated or blocked from the network. These include SIMs that were registered using fraudulent NINs. 11. Any dealer/agent blacklisted by a network for fraudulent SIM registration or SIM replacement transactions will be barred from all networks 12. The NCC will liaise with security agencies like EFCC and ONSA to block the accounts of any agent involved in fraudulently registered SIMs and NIN to serve as deterrent to others 13. The NCC will liaise with security agents to prosecute dealers/agents involved in fraudulently registered SIMs and NIN 14. Any Communications Service Provider that contravenes these guidelines will be sanctioned by the NCC. 15. Agents and Dealers must ensure that subscribers are not registered with multiple NINs and each subscriber shall only be registered with one NIN.
--	--	--

PART VII: SIM REGISTRATION RESTRICTIONS

7.1 To ensure compliance with regulatory standards and prevent misuse, the following operational guidelines shall apply to SIM registrations per authorized device:

		Daily Registration Cap: - Maximum permitted SIM registrations per device: 100 per calendar day. Post-Threshold Verification: - After 50 registrations within a single day, all subsequent registrations must undergo manual visual inspection (eyeballing) by a certified operator to confirm validity. - Verification includes cross-checking subscriber documentation and ensuring alignment with national identity databases. Prohibition of Offline Registrations: - All SIM card Registration must be conducted through a system-integrated process done online in real-time to the Communication Service Provider Backend. - Offline registrations (Manual entry, deferred data uploads or paperbased methods are strictly prohibited. Registration Hours ☐ 06:00hrs-23:59hrs
--	--	--

		5. All authorized devices shall be restricted to a Geo-Fenced radius of 25 meters from their Commission-registered coordinates during operation or as may be determined by the Commission. • All authorized SIM Registration Agents must be biometrically captured (Facial, Fingerprint, and Verified NIN). • All SIM Registration devices should be biometrically locked at all times and can only be accessed by four (4) authorized Registration Agents using his or her biometric data (Facial or Fingerprint).
--	--	--

PART VIII: MSISDN BLOCKING, BLACKLISTING AND ACCESS LIMITATIONS FOR PERSON AND AGENTS

The objective of this part is to set out:

1. Clear procedures and rules for blocking and/or deactivating from the network:
 - a) Suspected and fraudulently registered SIMs, including those with fraudulent NINs and,
 - b) MSISDNs identified to have been used in illicit activities or suspected to have been used in illicit activities ie activities that are in contravention with these business rules or laws in operation in Nigeria such as but not limited to; Fraud, SIM boxing, cybercrimes, terrorism, theft etc.
2. Blacklist for Persons/Agents flagged for fraudulent SIM registration and restrictions on persons under investigation.

PROCEDURES AND RULES FOR BLOCKING AND/OR DEACTIVATING FROM THE NETWORK SUSPECTED AND FRAUDULENTLY REGISTERED SIMS AND MSISDN IDENTIFIED TO HAVE BEEN USED OR SUSPECTED TO HAVE BEEN USED IN ILLICIT ACTIVITIES

8.1 Registered SIMs		
This flow covers below scenario: SIMs suspected to have been fraudulently registered		
1.	Context	Whereby on reasonable ground suspicion is cast by the Commission or a recognised authority as to the validity of a registered SIM
	Verification Process Flow	Where there is reasonable suspicion on the validity of a registered SIM the following process shall apply: i. The Communications Service Provider shall seek approval from the Commission to block the SIM in question from their network whereby the request/order did not come from the Commission. ii. Upon approval by the Commission, the SIM shall be immediately blocked. iii. Notification shall be sent to the subscriber via email or any other secondary means to proceed to the nearest respective communications subscriber centre. iv. Subscriber shall be requested to revalidate their registration with the necessary requirements.

		v. On compliance with the above, the Communications Service Provider shall seek approval from the Commission before unblocking the SIM. vi. Whereby the Subscriber refrains from complying with the above, the rules as regards number churning will apply after the prescribed period of dormancy and registered accordingly on the TIRMS Platform.
--	--	---

8.2 Registered SIMs

This flow covers below scenario:

Fraudulently Registered SIMs

1.	Context	Whereby it has been determined by the Commission or a competent authority that the SIM in question was fraudulently registered
	Deactivation Process Flow	Where it has been determined that the SIM in question was fraudulently registered the following process shall apply: i. The Communications Service Provider shall seek approval from the Commission to immediately block and deactivate the SIM in question whereby the communication did not come from the Commission. ii. Upon approval by the Commission, the SIM shall be immediately blocked and deactivated and the number churned. iii. Note that all numbers in this regard shall be duly registered on the TIRMS Platform accordingly.

8.3 Fraudulent MSISDN

This flow covers below scenario:

SIMs suspected to have been used in illicit activities

1.	Context	Whereby a MSISDN is reasonably alleged by the Commission or a recognised authority to have been used in the perpetuation of an offence under any law in operation in Nigeria
	Blocking Process Flow	Where there is reasonable suspicion that a MSISDN was used to commit an offence under operation in Nigeria, the following process shall apply:

		i. The Communications Service Provider shall seek approval from the Commission to block the SIM in question whereby the communication did not come from the Commission. ii. Upon approval by the Commission, the SIM shall be immediately blocked. iii. A notification shall be sent to the respective subscriber via email or any other secondary means informing them of the allegation, initiating party and process implemented. iv. The Subscriber shall also be advised on a process to adopt in order to escalate to the Commission if unsatisfied or if the process lingers longer than necessary. v. This process on the respective MSISDN shall be referenced on the TIRMS platform. vi. Where the subscriber has been exonerated and it has been communicated to the Communications Service provider, the Communications Service Provider shall seek approval from the Commission before unblocking the SIM.
--	--	--

8.4 Fraudulent MSISDN

This flow covers below scenario:
SIMs used in fraudulent activities

1.	Context	Whereby a MSISDN has been determined by a competent authority to have been used in the perpetuation of an offence under operation in Nigeria.
	Deactivation Process Flow	Where it has been determined that the MSISDN in question was used in fraudulent activities, the following process shall apply: i. The Communications Service Provider shall seek approval from the Commission to immediately block and deactivate the SIM in question whereby the communication did not come from the Commission.

		ii. Upon approval by the Commission the SIM shall be immediately blocked and deactivated and the number churned. iii. Note that all numbers in this regard shall be duly registered on the TIRMS Platform accordingly.
--	--	---

BLACKLIST OF PERSON/AGENT FOR FRAUDULENT SIM REGISTRATION AND RESTRICTIONS FOR PERSONS UNDER INVESTIGATION

8.5 Blacklist of Persons/Agents

This flow covers below scenario:

Person/Agent identified to have been involved in fraudulent SIM registration.

1.	Context	Whereby a Person/Agent has been determined by a competent authority to have been involved in fraudulent SIM registration.
	Blacklist Process Flow	Where it has been determined that a Person/Agent is involved in fraudulent SIM registration, the following process shall apply to blacklist the number: i. The Communications Service Provider shall seek approval from the Commission to blacklist the Person/Agent whereby the communication did not come from the Commission. ii. Upon approval by the Commission the Person/Agent shall be immediately blacklisted. iii. Note that all blacklisted persons/agents in this regard shall be duly registered on the TIRMS Platform accordingly.

8.6 Restrictions for persons under investigation

This flow covers below scenario:

Restrictions to network access for persons under investigation

1.	Context	Whereby a person has been placed under investigation by a competent authority on reasonable suspicion of the perpetuation of illicit activities.
----	---------	--

	Deactivation Process Flow	Where a person is reasonably suspected of illicit activities , the following process shall apply: i. The Communications Service Provider shall seek approval from the Commission to restrict the access of the suspect to their communications network and the degree of restriction to be applied, whereby the communication did not come from the Commission. ii. Upon approval by the Commission, the Communications Service Provider shall immediately restrict the access of the suspect in accordance with the Commission's Directive. iii. Note that all numbers in this regard shall be duly registered on the TIRMS Platform accordingly.
--	---------------------------	---

APPENDIX 1: REQUIREMENTS OF THE SELF SERVICE KNOW YOUR CUSTOMER (KYC) SYSTEM

REQUIREMENTS OF THE SELF SERVICE KNOW YOUR CUSTOMER (KYC) SYSTEM

1. Access to GPS location information, SIM and IMEI must be requested as a condition to launch mobile application and must stay on whilst the app is being used.
2. Facial image quality must conform to NCC facial image quality specifications, ICAO specifications and ISO/IEC 19794-1 and ISO/IEC 19794-5 specifications including white/plain background on self KYC mobile application/online solution.
3. Face Matching:
 - a) All Licensees shall ensure:
 - i. Images captured by the Consumer should be clear, not blurry and well-exposed.
 - ii. There is exactly one primary subject present in a photo.
 - iii. The entirety of the face should be visible in an image without any cropping.
 - iv. Extracted face regions should be at least 200 pixels on the shortest edge for auditing purposes.
 - v. The region of the image containing the face should have sufficient contrast for auditing purposes.
 - b) The Licensee should be able to match faces despite varying facial expressions or other minor changes in appearance.
 - c) Published error rates for false Matching Rate (FMR) shall not exceed 1/50,000.
4. Liveness Checks and Anti-spoofing algorithms must be incorporated in self KYC application/online solution.
 - i. The system should have Presentation Attack Detection (PAD) and be able to determine if a biometric sample is being captured from a living subject present at the point of capture.
 - ii. The system should be able to detect photos, videos, masks, and other printed materials.
 - iii. The system should have the ability to prompt users to perform a challenge such as smiling, turning their head, blinking, or waving a hand, and evaluate the performance of the task.
5. The following reports are required to be provided for the system in line with ISO/IEC 19795-1 specifications:
 - i. Technology Testing Report of the accuracy of the biometric technology independently of any specific system utilizing it.
 - ii. Scenario Testing report of the system's performance under simulated operational conditions
 - iii. Operational Testing report of the system's performance in its intended operational environment, involving the actual users and the complete system as deployed (utilizing the operational verifications carried out using the system over a specified period of time post system commissioning as determined by the Commission).
6. The following performance metrics of the system is required to be reported weekly in line with the ISO/IEC 19795-1 standard:

- i. False Match Rate (FMR) which is the probability that the system incorrectly matches the input image to a non-matching image template in the database
- ii. False Non-Match Rate (FNMR) which is the probability that the system fails to match the input image to a matching template in the database.
- iii. The trade-offs between FMR and FNMR.
- iv. Throughput rate which is the speed of processing biometric samples.
- v. Failure to Enroll Rate (FER) which is the rate at which attempts to create a biometric reference fail.
- vi. Failure to Capture Rate (FCR) which is the system's inability to capture a usable biometric sample.
7. Subscriber identity verification process as stipulated in SIM Registration Business Rules 2022 must be strictly adhered to (i.e. NIN verification and facial matching) on mobile application/online solution.
8. One Time Password (OTP) must be incorporated in process as stipulated in SIM Registration Business Rules 2022 for mobile application/online solution. This is only applicable for active MSISDNs and shall not apply to barred MSISDNs.
9. Requirements for re-registration for mismatched biometrics must be incorporated in self KYC mobile application/online solution. These are:
 - i. Affidavit / Indemnification
 - ii. Frequently dialed numbers
 - iii. Last recharge
 - iv. Frequently visited websites/apps
 - v. Any other parameters that the Commission may specify from time to time.
10. Re-registrations carried out via the self KYC App or web must be indicated in the MNO's SIM Registration Data Base.
11. Dedicated customer care lines must be provided to address subscriber complaints arising from utilization of the Self KYC Application/online solution for SIM-NIN linkage.
12. Reporting logs must be submitted to the Commission on a weekly basis containing information in the template below:

S N	CONDITIONS	ONLINE/WEB	MOBILE APP
1.	SUBMITTED MSISDN	YES	YES
2.	SUBMITTED NIN	YES	YES
S N	CONDITIONS	ONLINE/WEB	MOBILE APP
3.	DATE NIN SUBMITTED	YES	YES
4.	TIME NIN SUBMITTED	YES	YES

5.	URL	YES	YES
6.	DATE OTP SENT	YES	YES
7.	TIME OTP SENT	YES	YES
8.	FREQUENTLY DIALLED Nos	YES	YES
9	LAST RECHARGE AMOUNT	YES	YES
10	FREQUENTLY VISITED WEBSITE/APPS	YES	YES
11	DATE PICTURE UPLOADED	YES	YES
12	TIME PICTURE UPLOADED	YES	YES
13	PICTURE % MATCH	YES	YES
14	MAC ADDRESS	YES	YES
15	IMEI	NO	YES
16	IMSI	NO	YES
17	MSISDN USED FOR DATA	NO	YES
18	GPS LOCATION	NO	YES
19	IP ADDRESS	YES	YES

13. Licensee must maintain a valid ISO27001 certification.
14. The Solution must have confirmation from an independent accredited test lab acceptable to the Commission of having met the ISO/IEC 30107-3 Presentation Attack Detection (PAD) standard within six (6) months from the date of institution of this standard and renewed every 2 years.

APPENDIX 2. GLOSSARY OF TERMS AND ABBREVIATIONS

1.	API	Application Programming Interface – a software intermediary allowing connectivity between NIMC/NCC Central Database/NIBSS and the Communications Service Provider system for the purpose of calling up a subscriber's NIN records for verification, harmonization and linkage of NIMC database with Communications Service Provider SIM Registration database.
2	Agent/Dealer	A licensee of the Commission engaged by a Communications Service Provider to represent it in subscriber subscription activities.
3	Biometrics	This shall include Finger Print and Facial Image of the Subscriber.
4	COMMUNICATIONS SERVICE PROVIDER	It is an entity licensed by the Commission to provide communications services in whole or in part within Nigeria or on a ship or aircraft registered in Nigeria.
5	Device Handler	An individual to whom a device has been assigned and is responsible for the onboarding of new subscribers via SIM registration.
6	Effective Verification	Use of biometrics (Facial Image) to verify subscriber ownership on the SIM Registration Database.
7	Facial Verification	This shall be done by Electronic Facial matching and subsequently by case management which includes eyeballing. Electronic Facial matching will be fully implemented on a cutoff date determined by the NCC.
8	Functional Data	These are relevant data which is used to determine whether the Subscriber is eligible for telecom service. This data will be retrieved by the Communications Service Provider from NIMC database for the purpose of its telecom operations with respect to the subscriber identity verification.
9	Limited Access	This shall mean limitation by a Communications Service Provider of communication services available to a Subscriber to receipt of calls and Short Message Services (SMS) and making of calls to emergency numbers and the Communications Service Provider's call center only. There shall be no access to data services.
10	Limited Service Status	Limitation by a Communications Service Provider of communication services available to a Subscriber to receive Short Message Services (SMS) or communication from the Communications Service Provider only to confirm NIN verification of the subscriber.

11	Licensee	Means a provider of Communications Services that utilizes a subscription Medium in the Federal Republic of Nigeria.
12	MSISDN	Mobile Station International Subscriber Directory Number
13	M2M	Machine to Machine
14	NIBSS	Nigeria Inter-Bank Settlement System
15	NIMC	National Identity Management Commission.
16	NIMC Foundational Data	This explains who the Subscriber is and shall include the data as stated in the NIMC Agreed and Approved Minimal Fields - Appendix 7 to this Business Rules; retrieved from the NIMC database during NIN verification.
17	NIN records	National Identification Number records of a Subscriber on the NIMC database.
18	NIS	Nigerian Immigration Service
19	NCC	Nigerian Communications Commission.
20	OTP	One Time Password
21	P1 Service Outage	Complete loss of service, without possible alternative e.g. the verification service (Search by NIN only or fingerprint) from NIMC is not available.
22	P2 Service Outage	Degraded service. Non-critical function or process becomes unusable or difficult to use having an operational impact. Example where some queries to NIMC API do not return images hence Communications Service Providers are unable to provide service to the subscribers
23	Primary Telecom Master	This is a minimum Executive Management level staff who shall bear the authorized responsibility for the MSISDNs for corporate use and provide the operational primary NIN representation.
24	Secondary Telecom Master	This is a staff of a Corporate subscriber who will be responsible for operational activities of the Corporate account based on authorization by the Corporate entity for the activated MSISDN, SIM Replacements, MNP etc. The primary telecom master is allowed to delegate operational activities to a secondary telecom master. This individual must also be nominated via an authorization letter from the corporate entity.
25	Secondary users	These are employees of Corporate Subscribers whose SIMs/Lines are associated and linked with Corporate subscriber and account.

APPENDIX 3. SERVICE OFFERINGS TO SUBSCRIBERS

1.	SERVICE LEVELS BETWEEN NIMC AND COMMUNICATIONS SERVICE PROVIDERS	Service Levels will be agreed between Communications Service Providers and NIMC and set out as an Annexure to ensure seamless service delivery from the NIMC.
2.	Limited Access Governance	i. With respect to P1 service outage issues, Communications Service Providers are to submit service level statistics via email to the designated NCC officials on a weekly basis. ii. Where NIMC Service availability degrades consistently below the agreed Service Level thresholds as determined and agreed between NIMC and Communications Service Provider for one week, which results in a P1 outage issue, the NCC shall subject to its assessment of the service degradation statistics submitted by Communications Service Providers, communicate via an email to Communications Service Providers to trigger implementation of the Limited Access activation work around to mitigate the impact of the service outages on SIM activations only. iii. This Limited Access activation work around would persist for a period of 14 days or until the service availability level is restored and maintained to expected service levels for one week and as authorized by the Commission. iv. Service availability will be measured by the Communications Service Providers via scripts that attempt calls to the NIMC verification API intermittently (10minutes interval standard) and log the outcome of the attempts with failure reasons. The logged outcomes will be used to generate reports and shared by all Communications Service Providers with the designated NCC officials and collated to ascertain the overall availability of the verification service on a weekly basis for decision making by the governance body highlighted in i above. v. All other service levels will also be tracked by the Communications Service Providers individually for continual improvement purposes with NIMC. vi. Following the commencement of the Limited Access workaround, Communications Service Providers are to share the details of NIN and MSISDN of subscribers put on Limited Access activation to the NCC for monitoring.
		vii. Limited Service shall apply in the period prior to the activation of Limited Access Activation

APPENDIX 4. COMMUNICATIONS SERVICE PROVIDER SERVICE LEVEL REQUIREMENT

Communications Service Provider Service Level Requirements – NIN Verification Service provided by NIMC to the Communications Service Providers

4.0. Introduction

The objective of this document is to outline the Service Level Requirements (SLR) of the Communications Service Provider as regards the NIN verification service. The outlined Service Level Requirements are expected to guide the development of the Service Level Agreement (SLA) with NIMC to ensure mutually beneficial engagement between the Communications Service Provider and NIMC.

The service objects or elements covered include but not limited to NIN verification response time, NIN verification response information completeness, Network Connectivity, API access.

4.1. Service Level Expectations

#	Service Level Name	Expected Service Level
1.	Service Availability	99% resolved within target timeframe
2.	Service Reliability – Count of Unscheduled Outages	3 outages per calendar quarter
3.	Resolution of Priority 1 (P1) incidents	No more than 2 SLA breaches per Quarter (refer to section 3.4 below for target incident resolution timeframes)
4.	Resolution of Priority 2 (P2) Incidents	95% resolved within target timeframe (refer to section 3.4 below for target incident resolution timeframes)
5.	Notification for planned downtime and changes	1. Minimum of 72 hours before the planned downtime for effective planning 2. Change notification period should not be less than Five working days. However, the notification period depends on complexity of the change required by the Communications Service Providers which period should not be less than ten working days. 3. Communications Service Providers to be notified as soon as possible for emergency changes and planned downtimes

NB:

1. If Service Availability degrades consistently below the 99% expected service level, over a period of one week, Communications Service Providers would be authorized by the relevant governance body to trigger the **Limited Access** activation work around to mitigate the impact of the service outages on activations. This work around would persist until the service availability level is restored and maintained to expected service levels for one week and as authorized by the governance body.
2. Service availability will be measured by the Communications Service Providers via scripts that attempt calls to the NIMC verification API intermittently (10-minutes interval standard) and log the outcome of the attempts with failure reasons. The logged outcomes will be used to generate reports and shared by all Communications Service Providers with the NCC secretariat and collated to ascertain the overall availability of the verification service on a weekly basis for decision making by the governance body highlighted in #1 above.
3. All other service levels will also be tracked by Communications Service Providers individually for continual improvement purposes with NIMC.

4.2. Incident Prioritization Scheme

4.3. Incident Severity Classifications Definitions

#	Incident Severity Level	Definition
i.	High Complete loss of service. Interruption, without possible <i>Significant Business Impact</i>	alternative, making a critical functionality or solution inaccessible. Incident impacts all users of affected systems, expected to cause financial loss and reputational damage to Communications Service Providers.
ii.	Medium Complete loss of service. Interruption, without possible <i>Moderate Business Impact</i>	alternative, making a critical functionality or solution inaccessible. Incident impacts all users of affected systems, expected to cause financial loss and reputational damage to Communications Service Providers.
iii.	Low Degraded service. Non-critical function or process becomes <i>Minimal Business Impact</i>	unusable or difficult to use having an operational impact, but with no direct impact on services availability. A workaround is available. Impacts all users of affected systems but not expected to cause any financial loss and reputational damage

4.4 Urgency Level Definition

The urgency level below defines the extent to which the incident's resolution can bear delay in terms of the reaction time.

#	Urgency Level	Urgency Level Definition
1.	High <i>Immediate / Urgent</i>	The damage caused by the incident increases rapidly with potential to be widespread. Work that cannot be completed by Communications Service Provider user is highly time sensitive. Several Communications Service Provider subscribers with VIP status are affected.
2.	Medium <i>Standard Response</i>	The damage caused by the incident increases considerably over time.
3.	Low <i>Normal Response</i>	The damage caused by the incident only marginally increases over time. Work that cannot be completed by Communications Service Provider user because of the incident is not time sensitive

4.5 Resolution Priority

Urgency	Impact / Severity			
	Incident Severity Urgency	High	Moderate	Low
	High Immediate/Urgent	P1	P1	P2
	Medium Standard Response	P1	P2	P2
	Low Normal Response	N/A	P2	P2

The Priority levels define how quickly the NIMC Support team should address an incident. The priority level accorded incidents are _____ dependent on impact and urgency as shown below:

4.6 Target Incident Response and Resolution Time Frames

Service Level Category	Time Frame
Incident response time	Priority 1: 10 clock minutes Priority 2: 30 clock minutes
Incident resolution time	Priority 1: 4 clock hours Priority 2: 8 hours

Based on the foregoing example of incidents and expected treatment are outlined below:

Incident	Urgency	Severity	Priority	Response Time	Resolution Time	Resolution Process
Complete loss of service, without possible alternative e.g. the verification service (Search By NIN or fingerprint) from NIMC is not available	High	High	P1	10 clock minutes	4 clock hours	Communications Service Provider would notify NIMC via email to verificationsupport@nimc.gov.ng and such would be treated as an incident.

Degraded service. Non-critical function or process becomes unusable or difficult to use having an operational impact. Example where some queries to	Medium	Moderate	P2	30 clock minutes	8 hours	Communications Service Provider would notify NIMC via email to verification-support@nimc.gov.ng , and such would be treated as an incident.
NIMC API do not return images hence Communications Service Provider are unable to provide service to the subscribers						

APPENDIX 5 – CONSENT RULES

Subscriber Consent for SIM Registration Update		
General Rules for Obtaining Consent from the Subscriber (Individual and Corporate)		
1.	Channels/Rules	i. Subscriber consent shall be mandatory in all cases of harmonization that requires updating subscriber's SIM Registration data records with the NIMC data records. ii. Such consent shall be obtained physically and or through any one of following self-service channels: • USSD; • Link via SMS; • Web portal; • Email; and • Self-care App. iii. Data Retention: Evidence/logs of consent received shall be stored for a minimum period of 2 years and shall be retrievable when required. iv. Communications Service Providers shall deploy best efforts to raise general subscriber awareness on how to link their SIM Registration records with their NIN records.

APPENDIX 6: – SAMPLE MESSAGES - USSD

1.	SAMPLE MESSAGES	(i) Do not match. Press 1 to consent to update your SIM records with Dear Subscriber, please be informed that your personal data contained in your National Identification Number and SIM records your NIN details, otherwise press 2 to exit and visit our stores for further details; (ii) Dear Subscriber, please note that your KYC record does not match with your National Identification Number records. Press 1 to consent to update your SIM records with your NIN details. 2 to exit and visit our stores for further details; (iii) Dear Subscriber, please note that your KYC record does not match with your NIN records. Press 1 to consent to update your SIM records with your NIN details. Press 2 to exit and visit our stores for further details; (iv) Dear Subscriber, please be informed that your personal data tied to your NIN does not match your KYC record on our network. Press 1 to opt in to give consent to update your KYC records. Press 2 to opt out. Messages to Subscribers may be delivered via a two-step process to enable Communications Service Providers get consent for specific update required. Harmonized consent form to be hosted on Communications Service Provider’s website and used as physical or digital form.
----	-----------------	---

APPENDIX 7: NIMC AGREED AND APPROVED MINIMAL DATA FIELDS

1. The following data shall be provided by the MNO's for verification;

S/N	Data Request
1	National Identification Number
2	Live Image
3	Unique ID

2. The following data will be returned to the MNOs

S/N	Data Response
1	First name
2	Middle name
3	Last name
4	Gender
5	Date of Birth
6	TEL Token
7	Request ID
8	Customer Image
9	Residential address (including LGA, State and Country of residence)
10	Place of Origin
11	Data Matching score

3. NIN for Corporate;

This API allows Mobile Network Operators (MNOs) to verify their customers' demographic information against the records in the NIMC database.

S/N	Data Request
1	National Identification Number (NIN)
2	First Name
3	Last Name
4	Date of Birth

Upon submission, the API cross-checks the provided information against the NIMC records associated with the given NIN. The response includes a **matching status for each field**, indicating whether the **first name, last name, and date of birth** provided match the corresponding entries in the official NIMC database.

This service helps MNOs ensure accurate customer data and compliance with regulatory standards.

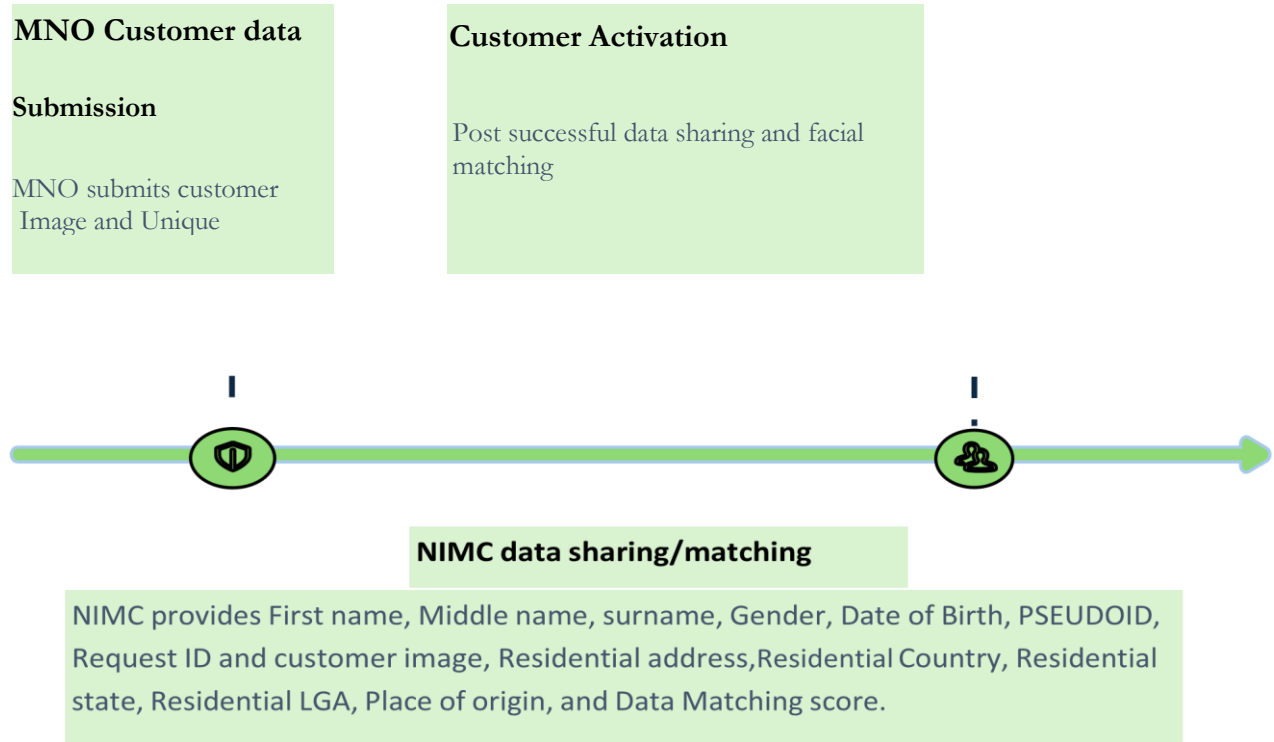
The following data shall be provided by the MNO's for verification

S/N	Data Request
1	National Identification Number
2	First name
3	Last name
4	Date of birth

The following data will be returned to the MNOs

S/N	Data Response	Response Value
1	Validated	True or False
2	First Name	Match or Not Match
3	Last Name	Match or Not Match
4	Date of Birth	Match or Not Match
5	NIN	Verified or Not Verified

The chart below shows the flow of the Customers Journey for the NIN Verification



APPENDIX 8: REQUIRED LIVENESS DETECTION AND FACIAL IMAGE STANDARDS

1. PURPOSE & SCOPE

This standard defines mandatory requirements for liveness detection and biometric image capture applicable to all NCC-licensed Operators, technology partners, and biometric partners. It sets the minimum acceptable security, quality, and compliance benchmarks for subscriber identity verification during Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap.

All Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap in Nigeria must use a single NCC liveness check standard. Independent implementations outside of this standard constitute a regulatory violation.

Liveness detection ensures the biometric is captured from a live human being physically present at the point of capture during Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap activities.

Governing standards: ISO/IEC 30107-3 · ISO/IEC 19794-5 · ISO/IEC 27001 · ICAO Doc 9303 · NDPR 2019 · NIST SP 800-63-4 · CEN/TS 18099:2024

2. LIVENESS DETECTION STANDARD

2.1 Recognized Liveness Types

- **Passive Liveness:** system detects liveness from natural micro-movements and texture analysis of a 3–5 second video stream — no user action required.
- **Active (Motion) Liveness:** applicant performs prompted actions such as eye blinks, head movement, or smile to validate KYC. Voice liveness is NOT required under this standard.
- **Hybrid Liveness:** combines passive and active (motion-based) methods. Most secure approach. Mandated for Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap.

2.2 Multi-Level Detection Architecture

Level	Location	Status
Option I — Primary	On-Device (Client-side)	Mandatory — all implementations
Option II — Secondary	Cloud / Server-side	Mandatory — all implementations

2.3. Mandatory Attack Vectors — Must Detect & Reject

Attack Type	Description	ISO/IEC 30107-3 Class
Print Attack	Photo or paper printout of a face	Presentation Attack Instrument (PAI)
Screen Replay Attack	Video played on phone, tablet, or monitor	Presentation Attack Instrument (PAI)
Mask Attack	Physical masks — 2D paper, 3D printed, silicone	Presentation Attack Instrument (PAI)
Deepfake/Synthetic	AI-generated or manipulated face	Presentation Attack Instrument (PAI)
Face Swap	Real-time digital face substitution	Presentation Attack Instrument (PAI)
Multiple Faces	More than one person in frame	Invalid Presentation
Partial/Occluded Face	Incomplete face or face cutout	Invalid Presentation

2.4. Injection Attack Detection (IAD)

- **Mandatory requirement:** All liveness check implementations must include a dedicated Injection Attack Detection (IAD) layer, separate from and complementary to the Presentation Attack Detection (PAD) layer. IAD is mandatory for all Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap events. Compliance with CEN/TS 18099:2024 is required at CEN Substantial level minimum; CEN High level is the target standard.
- **Scope of detection:** The IAD layer must detect and block attacks at the data stream level, including: (a) Injection Attack Method (IAM) — exploitation of software libraries, manipulation of network traffic, use of emulators, virtual cameras, and hooking into system functions to intercept and replace biometric data before it reaches the liveness engine; (b) Injection Attack Instrument (IAI) — synthetic faces, deepfake video sequences, and AI-generated images delivered via an established IAM.
- **IAD certification:** IAD conformance must be demonstrated by an ISO/IEC 17025-accredited independent laboratory against CEN/TS 18099:2024. Self-assessment is not permitted. Test reports must be submitted to NCC before deployment and renewed every 24 months or after any major model update. Partners must monitor and adopt ISO/IEC NP 25456 upon its publication as the international successor to CEN/TS 18099.

2.5 AI-Generated Content Detection (AIGCD)

- ▶ **Mandatory requirement:** All liveness check implementations must include a dedicated AI-Generated Content Detection (AIGCD) sub-module, operating as a distinct analytical layer from PAD and IAD. This module must specifically detect synthetic faces and manipulated biometric media produced by generative AI systems, including GAN-generated images, diffusion model outputs, neural face swaps, and AI-driven video manipulation. AIGCD is mandatory for all SIM Registration and SIM Swap events, in alignment with NIST SP 800-63-4.
- ▶ **Scope of detection:** The AIGCD module must analyse biometric media for artefacts and statistical signatures indicative of AI generation, including: GAN-generated faces (frequency-domain artefacts, blending boundaries, texture inconsistencies); diffusion model outputs (denoising artefacts, unnatural skin micro-texture); neural face swaps and face reenactment (temporal inconsistencies, boundary blending, lighting discontinuities); and AI-driven video manipulation (per-frame GAN signatures, unnatural blink patterns, audio-visual desynchronisation where applicable).
- ▶ **AIGCD performance thresholds:** Synthetic Face Rejection Rate $\geq 99\%$ across all tested generative AI attack types. Results must be reported per generation method (GAN, diffusion model, face swap, video manipulation). BPCER attributable to AIGCD controls must not exceed 1%. Detection must remain effective against publicly available generative AI tools and models.
- ▶ **Model currency:** Partners must maintain an active threat intelligence capability covering emerging generative AI attack methods. Where a new publicly available deepfake generation technique is identified and reported to NCC, partners must deploy a validated model update within 60 days of notification. Partners must submit a quarterly AIGCD model currency report to NCC documenting model version, training data vintage, and latest evaluation date.
- ▶ **AIGCD Output per Verification Event:** Each verification event must return an AIGCD Result (PASS / FAIL), an AIGCD Confidence Score (float 0-100), and a Synthetic Content Indicator (GENUINE / GAN_FACE / DIFFUSION_FACE / FACE_SWAP / VIDEO_MANIPULATION / UNKNOWN). All AIGCD signals must be included in the audit log. An AIGCD FAIL result must automatically block liveness approval and trigger a real-time fraud alert to the NCC.
- ▶ **Reporting:** All AIGCD FAIL events must be reported to NCC within 24 hours. Monthly AIGCD incident summaries must be included in the compliance report required under Section 8.3, including volumes, attack types detected, and model version in use at time of detection.

2.6 Technical Capture Requirements

- ▶ **Video:** 3–5 seconds · 1280×720 px (720p) recommended, 640×480 minimum · 24–30 fps · MP4/H.264 · max 10 MB (target 3–5 MB)
- ▶ **Head pose:** within $\pm 10^\circ$ pitch/roll/yaw for optimal results; maximum permitted deviation $\pm 15^\circ$; angle measurements as floating-point (2–6 decimal places)
- ▶ **Eyes:** both open and fully visible; confidence score for eyes open must exceed eyes closed; sunglasses and tinted lenses must be rejected; excessive reflection must be rejected

- ▶ **Mouth:** closed/neutral; confidence score for mouth closed must exceed mouth open; surgical masks, respirators, and facial coverings must be rejected
- ▶ **Face completeness:** full face forehead-to-chin visible; hair, hands, or objects must not obscure facial features
- ▶ **Image quality:** minimum 70/100 per ISO/IEC 19794-5 quality metric; composite score $\geq 75/100$; partner must document their quality scoring methodology

2.7 Required Output per Verification Event

- ▶ **Liveness Result:** Pass/Fail with numerical confidence score (Float 0–100)
- ▶ **Procedure Validation:** PASSED or FAILED
- ▶ **Face Genuineness:** GENUINE / PRINT_ATTACK / REPLAY_ATTACK / MASK_ATTACK / SYNTHETIC_FACE / FACE_SWAP / GAN_FACE / DIFFUSION_FACE / VIDEO_MANIPULATION / INJECTION_ATTACK
- ▶ **Multiple Face Flag:** SINGLE_FACE / MULTIPLE_FACES / NO_FACE — must block liveness if not SINGLE_FACE
- ▶ **Detection Level Applied:** PRIMARY / SECONDARY
- ▶ **Processing Time:** integer in milliseconds
- ▶ **Transaction ID:** UUID — unique per verification event
- ▶ **Confidence Thresholds:** threshold values at each confidence level for decision-making
- ▶ **Best Face Image:** highest-quality face extracted from video — Base64 encoded
- ▶ **Face Attributes:** quality scores, 3D head pose angles, eye status, mouth status
- ▶ **Attack Indicators:** all detected attack signals even at low confidence
- ▶ **PAD Scores:** APCER and BPCER per transaction
- ▶ **Geo-tag:** latitude and longitude at point of capture — mandatory
- ▶ **Subscriber ID:** hashed, linked to Subscriber reference record
- ▶ **Operator/Agent ID:** registered Operator agent identifier
- ▶ **Audit Log Hash:** SHA-256 cryptographic chain

2.8 Log Specification

- ▶ Transaction ID: Unique identifier (UUID format)
- ▶ Timestamp: ISO 8601 format in UTC (e.g., 2025-10-29T15:30:00Z)
- ▶ Subscriber ID: Unique subscriber identifier (hashed or encrypted for privacy)
- ▶ Verification Result: PASSED, FAILED, ERROR
- ▶ Confidence Score: Numerical confidence score (0-100)
- ▶ Procedure Validation: PASSED or FAILED
- ▶ Face Genuineness: GENUINE or attack type detected
- ▶ Multiple Face Detection: SINGLE_FACE, MULTIPLE_FACES, or NO_FACE
- ▶ Detection Levels Applied: PRIMARY, SECONDARY
- ▶ Processing Time: Time in milliseconds
- ▶ Device Information: Device model, OS version, app version
- ▶ Location: GPS coordinates
- ▶ Operator ID: ID of registration operator (if applicable)
- ▶ Registration Center: Registration center identifier (if applicable)
- ▶ Image Quality Scores: All ISO/IEC 19794-5 quality metric scores
- ▶ PAD Scores: APCER and BPCER scores if applicable

- ▶ Error Code: Specific error code if verification failed
- ▶ Attack Indicators: Any attack indicators detected
- ▶ Tamper-Evident Logging: All logs must be cryptographically hashed to ensure tamper-evidence
- ▶ Hash Chain: Implement hash chain where each log entry includes hash of previous entry
- ▶ Digital Signatures: Critical logs (breaches, configuration changes) must be digitally signed
- ▶ Write-Once Storage: Logs should be stored in write-once, read-many (WORM) storage
- ▶ Encryption: Logs containing sensitive data must be encrypted at rest
- ▶ Backup: Logs must be backed up daily to geographically separate location

3. PERFORMANCE THRESHOLDS

Standard	Requirement
Applicable Use Cases	Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap.
Required Liveness Method	Hybrid, Passive + Active (Motion-based).
Detection Architecture	Option I (On-Device) + Option II (Cloud), both mandatory.
APCER - Overall	< 1%
APCER - Print Attack	< 0.5%
APCER - Replay Attack	< 1%
APCER - Mask Attack	< 2%
BPCER	< 1%
False Acceptance Rate (FAR)	< 0.01%
False Rejection Rate (FRR)	< 1%
Liveness Detection Accuracy	> 99.5%
Face Comparison Accuracy	Minimum 80% confidence score required.
Face Comparison (Case Manager Review)	70-84% confidence, refer to case manager.
Processing Time	5-30 seconds end-to-end.
System Availability SLA	≥ 99.9%
Encryption - Transit	TLS 1.3, AES-256.
Encryption - At Rest	AES-256-GCM.

Standard	Requirement
Image Format	Base64, JPG (JPEG) or PNG; minimum 48×48 px; maximum 4096×4096 px; maximum 2 MB.
ISO 30107-3 & ISO 19794-5	Mandatory.
WCAG 2.2 Compliance	Level AA, Mandatory.
Data Retention	Minimum 2 years.

APCER = Attack Presentation Classification Error Rate. BPCER = Bona Fide Presentation Classification Error Rate. FAR = False Acceptance Rate. FRR = False Rejection Rate.

4. MANDATORY RULES

All Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap must comply with this standard. Non-compliance constitutes a regulatory violation.

- ▶ **Standard:** Hybrid Liveness — Passive + Active (motion-based)
- ▶ **AI engine:** single liveness check for Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap to operate liveness algorithms standards in implementation.
- ▶ **SDK/API:** standardised capture SDK or API deployed uniformly across all Operators and registration agents; may use XML or JSON with documented schema.
- ▶ **PAD Certification:** ISO/IEC 30107-3 PAD standard mandatory. Minimum conformance level: iBeta Level 2, tested by an NIST/NVLAP-accredited independent laboratory. Self-assessment is not permitted. A published roadmap to iBeta Level 3 conformance must be submitted to NCC within 12 months of deployment. APCER must be reported per attack species, not in aggregate only.
- ▶ **Geo-tagging:** latitude and longitude logged at every liveness event; independent from Operator-held records.
- ▶ **Audit logging:** all verification attempts — pass and fail — retained for 2 years minimum; logs encrypted at rest.
- ▶ **Accessibility:** WCAG 2.2 Level AA compliance mandatory; alternative authentication methods must be available.
- ▶ **Real-time monitoring:** security-relevant events must be monitored in real time; with dashboard access to NCC.
- ▶ **Partner documentation:** liveness check partner must provide technical documentation, system architecture, security documentation, and test results prior to deployment.

5. BIOMETRIC IMAGE CAPTURE STANDARD (ISO/IEC 19794-5 / ICAO Doc 9303)

5.1 Technical Specifications

Parameter	Recommended
Resolution	480 × 640 px or higher
Inter-pupil Distance	≥ 90 px
Minimum Distance between Pupils	64 pixels
Colour Depth	24-bit True Colour
Compression Image	JPEG / JPEG2000, maximum 15:1
Uncompressed Image	.BMP or .PNG
Min File Size	200 KB
Max File Size	5 MB
Aspect Ratio	3:4 Portrait
Colour Space	sRGB
Transmission	Base64 Encoded

5.2. Photographic Requirements (ICAO Doc 9303, Part 9)

Aspect	Requirement	Specification
Head Position	Frontal, centered	Maximum tilt $\pm 15^\circ$ (recommended $\pm 10^\circ$) pitch, roll, and yaw; front-to-back, side-to-side, and rotational movement limits apply.
Expression	Neutral	Mouth closed; no smiling or exaggerated expressions.
Eye Position	Open, at camera	Both eyes clearly visible and directed at the camera.
Eye Visibility	Fully visible	No hair, hands, or objects obstructing eyes or face.
Eye Image	Image Quality	• Both eyes must be visible • No excessive eyeglass reflection (it is preferable for quality assessment that no glasses are worn)
Eyewear	Minimal	Prescription glasses acceptable if there is no excessive reflection; dark/tinted lenses and sunglasses are not permitted.
Head Coverings	Not permitted*	Exception: religious or medical reasons only; face from chin to forehead must remain fully visible.
Lighting	Uniform, diffused	No harsh shadows or glare; 5000–6500K colour temperature recommended.
Shadows	None	No shadows on face or background.

Aspect	Requirement	Specification
Background	Plain, neutral	Grey or white; no patterns, objects, or other persons.
Camera Position	Eye level, perpendicular	Distance sufficient to capture head and shoulders (typically 1.5–2 metres).
Focus	Sharp	Clearly defined facial features; no motion blur.
Exposure	Properly exposed	No blown highlights or blocked shadows.

5.3 ISO/IEC 19794-5 Image Quality Metrics – Minimum 70/100 per metric; Composite Score ≥ 75/100

Quality Metric	Min Score	Measurement Method
Sharpness / Focus	80/100	Edge detection algorithms; frequency domain analysis
Illumination Uniformity	75/100	Standard deviation of pixel intensity across facial regions
Exposure Quality	75/100	Histogram analysis; dynamic range assessment
Dynamic Range	75/100	Histogram analysis; darkest-to-lightest tone range assessment
Colour Balance	75/100	White balance assessment; colour histogram analysis
Background Uniformity	75/100	Background region variance analysis
Overall Composite Score	75/100	Weighted average of all quality metrics above

6. DATA PROTECTION & PRIVACY

- ▶ **Legal basis:** Subscriber registration is a legal obligation; explicit subscriber consent must still be obtained before biometric collection.
- ▶ **Data minimization:** collect only biometric data strictly necessary for Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap.
- ▶ **Geo-tag independence:** NCC-held coordinates captured independently from Operator records, preventing remote spoofing.

7. OPERATOR CONTROL FRAMEWORK

The standardized governance, risk scoring, and fraud monitoring to be managed by the Operator, ensuring a zero-trust security model is uniformly enforced.

- ▶ **Real-time analytics:** live dashboard monitoring registration volumes, success rates, and fraud attempts
- ▶ **Geo-tag independence:** each Operator will hold coordinates captured independently from liveness check records, preventing remote spoofing and verifying physical agent presence.
- ▶ **Pattern analytics:** Operator shall capture anomaly detection and fraud trend in their report.

8. AUDIT & COMPLIANCE (ISO/IEC 27001)

8.1 Audit Log — Mandatory Fields per Transaction

Transaction ID (UUID) · UTC Timestamp · Subscriber ID (hashed) · Verification Result · Confidence Score · Face Genuineness State · Procedure Validation · Detection Level Applied · Processing Time (ms) · Device Information · GPS Coordinates · Operator ID · Registration Centre · ISO 19794-5 Quality Scores · PAD Scores (APCER/BPCER) · IAD Result · IAD Confidence Score · Injection Method Indicator · Sensor Integrity Flag · AIGCD Result · AIGCD Confidence Score · Synthetic Content Indicator · Attack Indicators · Error Codes

8.2 Log Integrity

- ▶ **Tamper-evidence:** SHA-256 hash chain — each entry includes the hash of the preceding entry.
- ▶ **Storage:** write-once (WORM); AES-256-GCM encrypted at rest; daily off-site backup.
- ▶ **Transmission:** TLS 1.3 minimum; all biometric data Base64 encoded in transit.
- ▶ **Access:** latitude and longitude coordinates logged for every verification event; access to logs restricted to authorized personnel only.

8.3 Reporting Obligations

Event	Requirement
Critical System Outage	Notify NCC within 24 hours.
New Vector Standard Identified	Notify NCC within 48 hours.
Liveness Check Complaints	Notify NCC within 72 hours.
Monthly Compliance Report	Submit to NCC, including volumes, PAD rates, incidents, and availability.

9. PARTNER CERTIFICATION & OPERATOR OBLIGATIONS

9.1 Pre-Deployment — All Criteria Mandatory

- ▶ **PAD Testing:** ISO/IEC 30107-3 PAD conformance demonstrated at iBeta Level 2 minimum by an NIST/NVLAP-accredited independent laboratory. APCER results must be submitted per attack species. A roadmap to iBeta Level 3 must be provided.
- ▶ **IAD certification:** Injection Attack Detection conformance demonstrated against CEN/TS 18099:2024 at CEN Substantial level minimum, by an ISO/IEC 17025-accredited independent laboratory. Test reports must be submitted to NCC before deployment. Partners must commit to achieving CEN High level within 24 months and to adopting ISO/IEC NP 25456 upon publication.
- ▶ **AIGCD capability:** AI-Generated Content Detection module demonstrated with Synthetic Face Rejection Rate $\geq 99\%$ per generation method (GAN, diffusion model, face swap, video manipulation). Test evidence covering all four generation method categories must be submitted to NCC before deployment. A quarterly model currency report schedule must be agreed with NCC prior to go-live.

- ▶ **Image quality:** ISO/IEC 19794-5 quality assessment capability demonstrated.
- ▶ **Accessibility:** WCAG 2.2 Level AA audit passed.
- ▶ **Data protection:** NDPR DPIA compliant
- ▶ **Security:** ISO/IEC 27001 logging demonstrated; penetration test and vulnerability assessment passed.
- ▶ **API/SDK:** HTTPS TLS 1.3; RESTful API + Native Mobile SDK + Mobile Web; auth via API Key, OAuth 2.0, or JWT.
- ▶ **Documentation:** technical documentation, system architecture, security documentation, and preliminary test results must be submitted before deployment.

9.2 Operator Obligations

- ▶ **Adopt the NCC-Liveness check standard** exclusively for all Subscriber Registration, Subscriber Re-registration, SIM Upgrade and SIM Swap.
- ▶ **Grant NCC unrestricted access** to real-time compliance dashboards and audit logs on request.

10. RESPONSIBILITY FOR COMPLIANCE WITH LIVENESS DETECTION AND FACIAL IMAGE STANDARDS

10.1 General Obligation

All Operators shall ensure that any liveness detection, facial biometric image capture or related technology deployed within their subscriber registration ecosystem fully complies with the prescribed specifications and standards.

10.2 Responsibility for Third-Party Compliance

Operators shall be fully responsible for ensuring compliance with the prescribed standards, notwithstanding that the liveness detection or facial biometric solution is provided by a third-party vendor, technology partner, or service provider.