STATUTORY INSTRUMENT

No. XX of 2026

SIM CARD REGISTRATION (AMENDMENT AND CONSOLIDATION) REGULATION 2026

Being a Regulation made under the **National Information and Communications Technology Act 2009** to amend and consolidate the **SIM Card Registration Regulation 2016** to:

a) integrate the **National Digital Identity Policy 2025** and **SevisPass Digital Identity and Trust Framework**;

b) designate a **Digital ID Implementation Authority** for eKYC and ongoing Customer Due Diligence (CDD);

c) enhance national security, data protection, consumer protection and financial integrity; and

d) give effect to Ministerial policy directions and **NEC Decision No. 183/2025** issued under Section 11 of the NICTA Act.

PART I – PRELIMINARY

1. Interpretation

(1) In this Regulation, unless the contrary intention appears:

"activate" means to enable full access to cellular electronic communications services, including the ability to make and receive calls and to send and receive messages and data.

"authorised personnel" means an officer or employee authorised by a licensee or by NICTA to perform specified duties associated with the subscriber information database or compliance with this Regulation.

"biometric information" means measurable physiological characteristics used for identity verification, including at minimum face, fingerprint and iris, in accordance with national biometric standards approved by Government.

"corporate body" includes a body corporate incorporated in or outside Papua New Guinea, a statutory authority, unincorporated association, partnership, or government department or agency.

"Customer Due Diligence" or "CDD" means ongoing identity verification and risk assessment processes, including periodic re-verification of subscriber identity, performed using SevisPass, SevisPass-Minor and SevisDEx in accordance with the Digital ID Trust Framework and applicable AML/CTF and financial sector standards.

"deactivate" means to disable a SIM Card's full access to a licensee's electronic communications network so that the SIM Card has only limited or no access as specified by this Regulation.

"Digital ID" means a digital identity credential issued under the National Digital Identity Policy 2025 and its associated Trust Framework.

"Digital ID Grace Period" means the period commencing on 1 January 2026 and ending on 30 June 2026, within which all existing subscribers must comply with the Digital ID linkage requirements of this Regulation.

"Digital ID Trust Framework" means the framework, rules, standards and procedures issued under the National Digital Identity Policy 2025 and enforced by NICTA as regulatory authority.

"Designated Digital ID Implementation Authority" means the entity designated under the National Digital Identity Policy 2025 and relevant NEC decisions to implement, operate and manage the SevisPass Digital Identity and Trust Framework, including SevisWallet, SevisDEx and associated eKYC and CDD services.

"electronic communications service" means a service that provides to users the ability to send or receive electronic communications, including voice, SMS, data and associated services.

"eKYC" means electronic know-your-customer identity verification undertaken using SevisPass, SevisPass-Minor and SevisDEx, in accordance with the Digital ID Trust Framework and applicable AML/CTF and financial sector standards.

"existing subscriber" means a subscriber on a licensee's electronic communications service system prior to the commencement of this amending Regulation.

"foreign licensee" means a telecommunications or electronic communications service provider licensed in a country other than Papua New Guinea.

"home country" means the country where a foreign licensee is established and operating from.

"ICT Appeals Panel" means the ICT Appeals Panel established under Section 255 of the NICTA Act.

"identification card" includes a driver's licence, employee card, citizenship card or other card evidencing identity, as may be prescribed.

"identification document" includes passports, birth certificates and any other documents evidencing identity, as may be prescribed.

"licensee" means a telecommunications or electronic communications service provider licensed by NICTA to provide electronic communications services in Papua New Guinea.

"limited access" means restricted access to services available to a SIM Card, limited to receipt of calls and messages and the making of calls to emergency numbers and the licensee's call centre.

"Minor Digital ID" or "SevisPass-Minor" means a digital identity credential issued to a person aged 13 to 17 years in accordance with the Digital ID Trust Framework, cryptographically linked to the SevisPass of a parent or legal guardian.

"new subscriber" means a subscriber who acquires or activates a SIM Card after the commencement of this amending Regulation.

"NICTA" means the National Information and Communications Technology Authority.

"NICTA Act" means the National Information and Communications Technology Act 2009.

"non-resident" means a visitor to Papua New Guinea who uses a SIM Card issued by a licensee or a foreign licensee roaming on a licensee's network.

"parent or legal guardian" means a person recognised as having parental, guardianship or custodial responsibility for a child or minor under applicable law.

"person" includes a natural person and a corporate body.

"personal information" means information relating to an identifiable person, including name, date of birth, gender, address, nationality, contact details and such other information as may be specified, subject to the Data Governance and Protection Policy and this Regulation.

"proxy registration" means a registration performed using the details of a person who is not the true holder or intended user of the SIM Card, except as expressly allowed in this Regulation for dependants.

"registration grace period" means the original 18-month period specified under the 2016 Regulation for first-time registration of existing subscribers, and does not limit or affect the later Digital ID Grace Period established by this Regulation.

"reputable person" means a person of standing in the community, including a Commissioner of Oaths, member of a disciplined force, ward member, village court magistrate, church pastor or other class of persons prescribed by NICTA, who is a registered SIM Card user and, where relevant, a SevisPass holder.

"SevisDEx" means the Government's secure data exchange and interoperability platform that enables trusted Digital ID verification and data sharing under the Digital ID Trust Framework.

"SevisPass" means Papua New Guinea's national sovereign Digital ID credential issued to persons aged 18 years and above in accordance with the National Digital Identity Policy 2025 and its Trust Framework.

"SevisWallet App" means the Government-approved application that provides the platform for SevisPass and SevisPass-Minor enrolment, management and authentication, and through which digital government services and SIM Card registration functions are delivered.

"security agency" means the Royal Papua New Guinea Constabulary or any other law enforcement or national security agency of the State, including the National Intelligence Organisation, as may be prescribed.

"SIM Card" means a Subscriber Identity Module smart card or embedded SIM associated with a telephone number and other network identifiers, used to access the services of a licensee.

"subscriber" means a person who subscribes to an electronic communications service as a result of the purchase or activation of a SIM Card or through a contract with a licensee, and includes both existing and new subscribers.

"subscriber information" means the minimum identity information, SevisPass, SevisPass-Minor or dependant linkage, and other data relating to a subscriber required to be collected and stored under this Regulation.

"subscriber information database" means the database established and maintained by a licensee containing subscriber information in accordance with this Regulation.

(2) Terms and expressions defined in the NICTA Act have the same meaning in this Regulation, unless the context otherwise requires.

PART II – OBJECTIVE AND APPLICATION

2. Objective

The objectives of this Regulation are to:

(a) provide a comprehensive regulatory framework for the registration, identification and ongoing management of all SIM Card users in Papua New Guinea;

(b) safeguard national security, public order, financial integrity and consumer protection by ensuring that all SIM Card users are uniquely and reliably identifiable;

(c) integrate SIM Card registration with the **National Digital Identity Policy 2025**, including SevisPass and SevisPass-Minor, as core components of the country's Digital Public Infrastructure;

(d) ensure that the collection and management of subscriber information comply with national data governance, data protection and cybersecurity policies; and

(e) support risk-based **electronic know-your-customer (eKYC)** and ongoing **Customer Due Diligence (CDD)** processes for SIM Card holders, consistent with national AML/CTF obligations and financial inclusion objectives, through the Designated Digital ID Implementation Authority.

3. Application

(1) This Regulation applies to all licensees operating in Papua New Guinea and to all persons who use a SIM Card issued by a licensee in Papua New Guinea.

(2) This Regulation does not apply to users of SIM Cards issued by foreign licensees roaming on a licensee's network, except as provided under provisions relating to non-residents.

PART III – SUBSCRIBER INFORMATION DATABASES AND DATA PROTECTION

4. Establishment and maintenance of subscriber information databases

(1) Each licensee shall establish and maintain a subscriber information database to record and store subscriber information in accordance with this Regulation.

(2) The subscriber information database shall be hosted and maintained within the territory of the Independent State of Papua New Guinea, unless otherwise authorised by law.

(3) Ownership, care and control of the subscriber information database, subject to this Regulation and the NICTA Act, rest with the licensee.

5. Data protection, confidentiality and data minimisation

(1) Subscriber information is confidential. No person may access subscriber information except as authorised under this Regulation or any other law.

(2) Licensees must adopt **data minimisation** principles and must not collect or store raw biometric information of subscribers, except where explicitly authorised by law and in accordance with the Digital ID Trust Framework.

(3) Identity verification for SIM registration and ongoing compliance shall be conducted through SevisPass or SevisPass-Minor, via the SevisWallet App and SevisDEx. Licensees shall store only:

(a) the relevant Digital ID identifier or verification token;
(b) the SIM Card identifier and MSISDN;
(c) activation and status information; and
(d) such limited metadata as may be prescribed by NICTA.

(4) Licensees shall implement appropriate technical and organisational measures, including encryption, access control, logging and audit trails, to preserve the integrity, confidentiality and availability of subscriber information.

(5) Licensees shall promptly notify NICTA and affected subscribers of any material data breach in accordance with procedures issued by NICTA.

(6) A licensee that uses subscriber information for any unauthorised commercial or other purpose commits an offence and is liable to a fine not exceeding K50,000 per subscriber, in addition to forfeiture of any commercial benefit obtained.

6. Use and retention of subscriber information

(1) Subscriber information shall be used solely for:

(a) compliance with this Regulation and the NICTA Act;
(b) provision, billing and maintenance of electronic communications services; and
(c) compliance with lawful requests from security agencies.

(2) When a SIM Card is deactivated, the licensee shall retain the relevant subscriber records for a minimum of six months, or such longer period as may be prescribed, and thereafter securely destroy or irreversibly anonymise such records, unless retention is required by law.

7. Requests for subscriber information by security agencies

(1) Subscriber information may be provided to a security agency only in response to a written request that:

(a) is in the prescribed form;
(b) states the rank and authority of the requesting officer;
(c) sets out the legal basis and purpose of the request; and
(d) is endorsed in accordance with any procedure approved by NICTA and relevant authorities.

(2) A licensee shall refuse any request that would breach the Constitution, any Act of Parliament or would constitute a threat to national security as advised by competent authorities.

(3) A licensee that transmits subscriber information to an unauthorised person or without proper authorisation commits an offence and is liable to a fine not exceeding K50,000 for each affected SIM Card.

PART IV – SIM CARD REGISTRATION AND AGE STRUCTURE

8. General obligation to register subscribers

(1) Every licensee shall ensure that every SIM Card on its network is registered in accordance with this Regulation.

(2) A licensee shall not activate a SIM Card unless the subscriber has complied with the identification and Digital ID requirements under this Regulation.

9. Registration of adult subscribers (18 years and over)

(1) A person aged 18 years or over may be registered as a subscriber only if the person holds a valid SevisPass.

(2) Registration shall be carried out by the subscriber using the SevisWallet App, utilising its SIM Registration function, or by authorised assisted-registration using tools integrated with SevisWallet, in the presence of the subscriber.

(3) Initial identity verification at onboarding for a person aged 18 years or over shall be conducted by means of **eKYC** using SevisPass through SevisWallet and SevisDEx, delivered by the Designated Digital ID Implementation Authority.

(4) A licensee shall not activate or maintain a SIM Card in the name of a person aged 18 years or over unless:

(a) the subscriber's SevisPass has been issued;
(b) eKYC has been successfully completed; and
(c) the SIM Card is linked to that SevisPass and the linkage has been verified through SevisDEx.

10. Registration of corporate subscribers

(1) For a corporate body, the licensee shall register:

(a) the corporate body's name, registered office and registration number (where applicable); and
(b) the SevisPass details of at least one authorised representative who will be responsible for the SIM Card(s) of the corporate body.

(2) Initial identity verification of authorised representatives shall be conducted by means of eKYC using SevisPass through SevisWallet and SevisDEx.

(3) The SIM Cards of a corporate body shall be linked to the SevisPass of its authorised representative(s) through the SevisWallet App or an approved system integrated with SevisDEx.

11. Registration of new subscribers generally

(1) A new subscriber, whether an adult, minor or dependant, shall at the time of acquiring and activating a SIM Card comply with the applicable age-based identification and Digital ID rules set out in this Part.

(2) A licensee shall not activate a SIM Card for any new subscriber unless the relevant SevisPass, SevisPass-Minor or dependant linkage requirements have been fulfilled, and eKYC has been completed where required, and verified through SevisDEx.

12. Digital ID requirements for minors (13–17 years)

(1) A person aged 13 to 17 years may be registered as a subscriber only if the person is issued a Minor Digital ID credential (SevisPass-Minor) through the SevisWallet App in accordance with the Digital ID Trust Framework.

(2) A SevisPass-Minor shall:

(a) contain identity attributes appropriate for a minor;
(b) be cryptographically linked to the SevisPass of a parent or legal guardian; and
(c) be subject to parental or guardian oversight as prescribed under the Digital ID Trust Framework.

(3) Initial identity verification at onboarding for a person aged 13 to 17 years shall be conducted by means of eKYC using SevisPass-Minor through SevisWallet and SevisDEx.

(4) A licensee shall not activate or maintain a SIM Card in the name of a person aged 13 to 17 years unless:

(a) a SevisPass-Minor has been validly issued;
(b) eKYC has been successfully completed; and
(c) the SIM Card is linked to the SevisPass-Minor and the linkage has been verified through SevisDEx.

(5) Upon the subscriber attaining 18 years of age, the SevisPass-Minor shall be transitioned to a full SevisPass and the subscriber shall assume full ownership and responsibility for any associated SIM Card(s).

13. Registration of children aged 12 years and below

(1) A child aged 12 years or below shall not be registered as a subscriber in their own name.

(2) Any SIM Card used by a child aged 12 years or below must be registered under the SevisPass of a parent or legal guardian, who shall be responsible for the SIM Card and all activities conducted using it.

(3) For children aged 12 years and below:

(a) the SIM Card shall be recorded in SevisWallet as a **Dependent SIM**; and
(b) the parent or guardian shall have full oversight over usage and status of the Dependent SIM.

(4) A licensee shall not activate or maintain a SIM Card intended for use by a child aged 12 years or below unless the SIM Card is linked to the SevisPass of a parent or legal guardian through SevisWallet or an authorised assisted-registration channel.

14. Responsibilities of parents and guardians

(1) A parent or legal guardian whose SevisPass is linked to a SevisPass-Minor or a Dependent SIM is responsible for:

(a) verifying the identity of the child or minor;
(b) approving activation and ongoing use of the child's or minor's SIM Card;
(c) supervising the usage and safety of the service; and
(d) promptly reporting any misuse, loss or unauthorised activity to the licensee.

(2) A parent or guardian shall not permit a child or minor to use a SIM Card registered in the name of a person who is not the parent, guardian or the minor themself (where permitted under this Regulation).

15. Registration of non-residents

(1) A non-resident who purchases a SIM Card from a licensee shall, at the time of registration:

(a) present a valid passport or travel document; and
(b) provide local contact details and such other information as may be prescribed.

(2) Where enabled by policy and technology, non-residents may be issued a limited or guest Digital ID for the purposes of SIM registration, in accordance with the Digital ID Trust Framework.

16. Limit on active SIM Cards

(1) An individual subscriber may hold no more than six active SIM Cards across all licensees, unless otherwise prescribed by NICTA.

(2) Licensees shall use SevisPass, SevisPass-Minor and dependant linkage information to ensure compliance with this limit.

17. Prohibition of unauthorised minor usage

(1) No SIM Card shall be used by a person aged 13 to 17 years unless linked to a valid SevisPass-Minor in accordance with this Regulation.

(2) No SIM Card shall be used by a child aged 12 years or below unless registered as a Dependent SIM linked to the SevisPass of a parent or legal guardian.

(3) A licensee that knowingly permits unauthorised minor usage contrary to this section commits an offence and is liable to penalties under this Regulation.

PART IVA – SEVISPASS DIGITAL ID, IMPLEMENTATION AUTHORITY AND COMPLIANCE

18. Recognition of SevisPass and SevisPass-Minor

(1) SevisPass, issued through the SevisWallet App, is recognised as the mandatory Digital ID credential for:

(a) registration and ongoing use of SIM Cards by persons aged 18 years and over; and
(b) registration of corporate subscribers through their authorised representatives.

(2) SevisPass-Minor, issued through the SevisWallet App, is recognised as the mandatory Digital ID credential for registration and ongoing use of SIM Cards by persons aged 13 to 17 years.

19. Designated Digital ID Implementation Authority and eKYC/CDD services

(1) The Designated Digital ID Implementation Authority is responsible for:

(a) implementing and operating the SevisPass Digital Identity and Trust Framework;
(b) operating SevisWallet and SevisDEx for Digital ID issuance, authentication and verification; and

(c) providing eKYC and CDD services to licensees and other relying parties for SIM registration and ongoing subscriber identity management.

(2) For the purposes of SIM Card registration and compliance with this Regulation:

(a) all initial identity verification of new subscribers shall be conducted by means of **eKYC** using SevisPass or SevisPass-Minor through SevisWallet and SevisDEx; and
(b) all periodic identity re-verification required under this Regulation shall be conducted by means of **CDD** using SevisPass or SevisPass-Minor through SevisWallet and SevisDEx.

(3) The Designated Digital ID Implementation Authority may **levy fees** on licensees for the provision of eKYC and CDD services required under this Regulation.

(4) The structure and level of eKYC and CDD fees shall:

(a) be set out in a schedule published by the Designated Digital ID Implementation Authority;
(b) be subject to review and approval by NICTA, in consultation with the Department of ICT and relevant economic regulators, as appropriate; and
(c) be applied on a **non-discriminatory** basis to all licensees.

(5) NICTA may impose additional regulatory conditions on eKYC and CDD pricing, including caps or pass-through rules, to protect consumers and ensure that fees are reasonable and cost-based.

20. Digital ID Grace Period for existing subscribers

(1) A Digital ID Grace Period is declared from 1 January 2026 to 30 June 2026.

(2) During the Digital ID Grace Period:

(a) all existing subscribers aged 18 years and over must obtain a SevisPass (if they do not already hold one) and link each of their active SIM Cards to their SevisPass using the SevisWallet App or authorised assisted-registration channels;
(b) all existing subscribers aged 13 to 17 years must obtain a SevisPass-Minor and link each of their active SIM Cards to their SevisPass-Minor; and
(c) all SIM Cards used by children aged 12 years and below must be linked as Dependent SIMs to the SevisPass of a parent or legal guardian.

(3) During the Digital ID Grace Period, licensees shall:

(a) provide subscribers with free and reasonable means, including digital and assisted channels, to complete the required enrolment and linkage;
(b) send periodic SMS and other notifications to subscribers informing them of the requirements and deadlines; and
(c) report monthly to NICTA on progress towards compliance in the form and manner prescribed by NICTA.

21. Deactivation of non-compliant SIM Cards after the Digital ID Grace Period

(1) After 30 June 2026, a licensee shall deactivate any SIM Card that:

(a) is not linked to a valid SevisPass, SevisPass-Minor or Dependent SIM arrangement, as applicable; or
(b) is linked to a SevisPass or SevisPass-Minor that has been revoked, suspended or otherwise invalidated under the Digital ID Trust Framework.

(2) A licensee that fails to deactivate a non-compliant SIM Card in accordance with Subsection (1) commits an offence and is liable to a fine not exceeding K50,000 for each non-compliant SIM Card, in addition to any penalty under the NICTA Act.

(3) A deactivated SIM Card may be reactivated only after the subscriber has:

(a) obtained or restored a valid SevisPass or SevisPass-Minor, or established a valid Dependent SIM linkage; and
(b) completed the SIM linkage and verification process through SevisWallet and SevisDEx.

22. Annual Customer Due Diligence for active SIM Cards

(1) In addition to the initial eKYC undertaken at onboarding, each licensee shall ensure that **every active SIM Card** on its network is subject to at least one **Customer Due Diligence (CDD)** identity re-verification every twelve (12) months, using SevisPass or SevisPass-Minor through SevisWallet and SevisDEx.

(2) Annual CDD may be triggered by:

(a) a scheduled background check executed by the licensee through SevisDEx;
(b) a significant account event, including major profile changes, SIM replacement, migration from prepaid to post-paid, or other events specified by NICTA; or
(c) any other trigger defined by NICTA or the Designated Digital ID Implementation Authority.

(3) The Designated Digital ID Implementation Authority may charge licensees a fee for each CDD check performed under this section, in accordance with the approved fee schedule under Section 18A.

(4) Where a subscriber fails or does not complete the required annual CDD:

(a) the licensee shall place the relevant SIM Card into limited access and notify the subscriber that CDD is overdue;
(b) if the subscriber does not complete CDD within a period specified by NICTA (which shall not be less than thirty (30) days from the date of notification), the licensee shall deactivate the SIM Card; and
(c) the SIM Card may only be reactivated after successful completion of CDD and verification through SevisPass or SevisPass-Minor.

(5) Licensees shall maintain audit logs and CDD records for each SIM Card for such period as may be specified by NICTA, and shall make these records available to NICTA upon request for inspection or audit.

(6) NICTA may issue further rules on:

(a) the scheduling and batching of CDD checks;
(b) prioritisation of higher-risk subscriber segments; and
(c) coordination of CDD requirements with other AML/CTF or sectoral requirements to avoid duplication and unnecessary cost.

23. Interoperability, fees and consumer protection

(1) All licensees shall integrate their subscriber registration and management systems with SevisDEx and the Digital ID Trust Framework in accordance with technical standards issued by NICTA.

(2) The costs associated with the development, integration and maintenance of interoperability for SIM–Digital ID linkage shall be shared among licensees in such manner as NICTA may determine, having regard to Ministerial policy directions and NEC decisions.

(3) Licensees shall not impose any charge on subscribers for:

(a) initial SevisPass or SevisPass-Minor enrolment; or
(b) the mandatory SIM–Digital ID linkage required as a condition of compliance with this Regulation.

This does not prevent the Designated Digital ID Implementation Authority from levying fees on licensees for eKYC and CDD services under Section 18A, nor does it prevent NICTA, in consultation with relevant stakeholders, from determining whether and how licensees may recover such costs as part of their regulated tariffs.

(4) NICTA may issue additional consumer protection rules to ensure that any cost recovery by licensees is transparent, reasonable and consistent with broader competition and consumer policy.

24. Policy alignment

In administering this Regulation, NICTA and licensees shall give effect to:

(a) the National Cyber Security Policy 2021;
(b) the Data Governance and Protection Policy 2024; and
(c) the National Digital Identity Policy 2025 and the SevisPass Digital Identity and Trust Framework.

PART V – REGISTRATION UPDATES, INSPECTION AND REPORTING

25. Registration updates

(1) Licensees shall, at intervals specified by NICTA, submit updated subscriber registration and Digital ID linkage information to NICTA in the prescribed form.

(2) A licensee that fails to provide the required information after a written warning from NICTA commits an offence and is liable to a fine not exceeding K50,000.

26. Inspection, audits and NEC reporting

(1) NICTA may carry out inspections, audits and system tests on licensees to ensure compliance with this Regulation.

(2) Licensees shall provide reasonable assistance and access to NICTA for the purposes of inspections, audits and system tests.

(3) NICTA shall submit quarterly reports to the Minister and to the National Executive Council on the status of implementation of this Regulation, including progress on SevisPass and SevisPass-Minor adoption, SIM–Digital ID linkage, eKYC and CDD coverage, as required under Ministerial Section 11 directions.

PART VI – PENALTIES AND APPEALS

27. General penalties

(1) Without prejudice to other penalties under any law, a licensee or person who contravenes a provision of this Regulation for which no specific penalty is provided commits an offence and is liable to a fine not exceeding K50,000.

(2) Where an offence is committed by a corporate body, any director, chief executive officer, manager, secretary or similar officer who authorised, permitted or failed to prevent the offence may also be held personally liable, unless that person proves that they exercised all reasonable precautions and due diligence to prevent the commission of the offence.

27. Appeals

(1) A licensee aggrieved by a decision or fine imposed by NICTA under this Regulation may appeal to the ICT Appeals Panel in accordance with the NICTA Act.

(2) The decision of the ICT Appeals Panel shall be final, subject to any right of review or appeal provided by law.