No. of 2026

***Verifiable Credential and Trust Services Bill* 2026.**

Certified on:

(national crest)

No. of 2026

ARRANGEMENT OF SECTIONS.

***Verifiable Credential and Trust Services Bill* 2026.**

(national crest)

No. of 2026

A BILL FOR AN ACT

entitled

***Verifiable Credential and Trust Services Act* 2026.**

Being an Act to –

(a) establish the legal foundation for Papua New Guinea's National Digital Trust Ecosystem, encompassing digital identity, verifiable credentials, trusted data exchange, and digital payments;
(b) recognise SevisPass as the foundational digital identity credential within that ecosystem;
(c) provide for the issuance, holding, management, presentation, verification, suspension, revocation and legal recognition of verifiable credentials through approved digital wallets and trust services;
(d) establish a national National Digital Identity and Trust Services Framework;
(e) provide for the designation of a regulatory authority, as an independent statutory regulator, and an implementation authority;
(f) provide for accreditation, oversight, privacy, data protection, compliance, enforcement, appeals, regulations, transitional and savings matters; and
(g) make consequential amendments to related Acts,

and for related purposes.

MADE by the National Parliament to come into operation –

(a) Subject to Subsections (b), (c) and (d) below, on the date on which it is certified by the Speaker as having been made by the National Parliament.

(b) The following provisions shall come into operation on the date of certification under Subsection (a) above:

i. Part I;
ii. Part VI;
iii. Part VII; and
iv. the savings and transitional provisions specified in Part IX.

(c) The following provisions shall come into operation on a date fixed by the Minister by notice in the National Gazette:

i. Part II;
ii. Part III;
iii. Part IV;

iv. Part V;
v. Part VIII; and
vi. Schedule 1 to the extent necessary for staged implementation.

(d) Any provision of this Act not brought into operation under Subsection (c) shall come into operation no later than 36 months after the date of certification, unless the National Executive Council otherwise directs on the advice of the Minister by decision published in the National Gazette.

(e) Different dates may be fixed for different provisions and for different classes of persons, credentials, sectors, transactions or entities.

PART I. — PRELIMINARY

1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS

[*to be completed in consultation with the State Solicitor*]

2. OBJECTS OF THIS ACT

(1) The objects of this Act are to establish the legal foundation for Papua New Guinea's National Digital Trust Ecosystem, providing a comprehensive framework that enables trusted, secure, interoperable, and legally recognised digital interactions across the public and private sectors, encompassing Trust Services and the complete lifecycle of a trusted digital transaction, including—

(a) digital identity authentication through SevisPass or any other Recognised Verifiable Credentials;

(b) the issuance, exchange, presentation, verification, suspension, revocation, and storage of verifiable credentials within secure digital wallets;

(c) trusted data exchange through SevisDEx, the national secure data exchange platform, or other accredited trust services; and

(d) the secure execution of digital payments through SevisPay or other accredited payment systems and gateways.

(2) This Act establishes and maintains a legally robust, technologically secure, and operationally resilient National Digital Identity and Trust Services Framework that governs the operation of the National Digital Trust Ecosystem and provides assurance to individuals, government agencies, relying parties, accredited trust service providers, and private sector participants regarding the authenticity, integrity, confidentiality, interoperability, availability, revocation status, and legal effect of digital identities, verifiable credentials, trust services, and digital transactions.

(3) This Act protects the rights, privacy, security, consent, and autonomy of individuals while enabling trusted, user-centric, interoperable, and privacy-preserving digital interactions that

support innovation, Digital Public Infrastructure, digital government, digital commerce, financial inclusion, and the broader digital economy.

(4) This Act establishes a comprehensive governance, accreditation, assurance, compliance, supervisory, and enforcement regime for all participants operating within the National Digital Trust Ecosystem. Responsibility for regulating and overseeing the ecosystem is vested in the Regulator designated under Section 26, an independent statutory regulator, with powers to establish standards, accredit trust service providers, monitor compliance, enforce the provisions of this Act, and maintain the integrity and public confidence of the National Digital Trust Ecosystem.

(5) This Act, together with any regulations, rules, standards, codes, determinations, or decisions made under it, shall be interpreted and administered in a manner that promotes trust, legal certainty, interoperability, innovation, technology neutrality, security, and public confidence in Papua New Guinea's National Digital Trust Ecosystem, ensuring that trusted digital interactions are recognised and enforceable throughout their entire lifecycle.

3. CONSTITUTIONAL AND RIGHTS SAFEGUARDS

(1) This Act shall be interpreted, so far as possible, in a manner consistent with the constitutional rights of residents of Papua New Guinea, including the right to privacy under Section 49 of the Constitution.

(2) Any limitation on privacy, liberty, access, use, suspension, revocation, verification or disclosure under this Act shall be—

(e) prescribed by law;

(f) reasonably necessary and proportionate to a legitimate public purpose; and

(g) subject to safeguards, including notice, reasons, review and appeal where applicable.

(3) No person shall be denied access to an essential government service solely on the ground that the person does not hold SevisPass.

4. INTERPRETATION

In this Act, unless the contrary intention appears—

"accredited issuer" means an entity accredited by the Regulator under this Act to issue verifiable credentials within the National Digital Identity and Trust Services Framework;

"accredited partner" means an entity accredited by the Regulator to participate in the National Digital Identity and Trust Services Framework in a category prescribed by this Act or the regulations;

"approved digital wallet" means a digital application or service approved by the Regulator for the holding, management, storage, presentation or verification of verifiable credentials under this Act;

"Approved Payment System, Gateway or Digital Payment Service" means a payment system, gateway or digital payment service approved by the financial Regulator for the secure execution of digital payments within the National Digital Trust Ecosystem, and includes SevisPay while so approved;

"Approved Trust Service Provider" means a person or entity approved or accredited by the Regulator to provide a Trust Service within the National Digital Trust Ecosystem;

"authorised issuer" means a public body authorised by or under this Act or another written law to issue a verifiable credential within the National Digital Identity and Trust Services Framework;

"biometric data" means biometric information within the meaning of the *Civil and Identity Registration Act* 2024 or, where not defined there, data derived from a person's physical, physiological or behavioural characteristics that permits or confirms unique identification;

"continuity of service" means the uninterrupted availability, or prompt restoration, of SevisPass, SevisWallet, approved digital wallets, the Trust Registry, SevisDEx and other critical components of the National Digital Trust Ecosystem, and of a holder's access to and use of the holder's verifiable credentials, notwithstanding a change of Implementation Authority, accredited partner, technology or infrastructure or service provider;

"credential schema" means the approved data structure, format, minimum attributes, encoding rules and validation requirements for a category of verifiable credential;

"credential holder" or "holder" means a natural person to whom a verifiable credential has been issued and in whose approved digital wallet it is held or managed;

"Department" means the department responsible for information and communications technology;

"National Digital Identity and Trust Services Framework" means the legal, technical, operational and institutional framework established by this Act for the National Digital Trust Ecosystem, including standards, governance arrangements, trust registry arrangements, accreditation, supervision and approved trust services;

"National Digital Identity and Trust Services Framework Implementation Authority" means the entity designated under Section 30;

"Regulator" means the entity for the time being responsible for the regulation of information and communications technology and the digital economy, designated under

Section 26 as the regulator for the purposes of this Act, and includes the National Information and Communications Technology Authority while so designated;

"essential government service" means a public service prescribed by regulation or declared by the Minister, after consultation with relevant agencies, to be essential for access to basic public administration, civil status, health, education, social protection, emergency services or justice;

"material system failure" means a failure, outage, degradation or compromise of a system, platform or infrastructure forming part of the National Digital Trust Ecosystem that—(a) prevents or materially impairs the issuance, presentation, verification, suspension or revocation of verifiable credentials; (b) affects a significant number of holders, authorised issuers, accredited partners or relying parties; or (c) threatens the integrity, availability or confidentiality of the Trust Registry or another critical system, for a period, or of a severity, prescribed by regulation;

"Minister" means the Minister responsible for Information and Communications Technology;

"National Digital Trust Ecosystem" means the operational environment governed by the National Digital Identity and Trust Services Framework, comprising individuals, government agencies, private sector entities, relying parties, Recognised Verifiable Credential Issuers, Approved Trust Service Providers, accredited technology and infrastructure providers and other participants prescribed under this Act, supporting trusted digital interactions across government, commerce, financial services and the broader digital economy;

"national security" means the defence, sovereignty, territorial integrity and security of Papua New Guinea and its people, and includes the protection of Papua New Guinea and its critical infrastructure, including the National Digital Trust Ecosystem, against espionage, sabotage, terrorism, foreign interference and other threats to the safety of the State, to be read consistently with Section 38 of the Constitution;

"NICTA" means the National Information and Communications Technology Authority established under the *National Information and Communications Technology Act* 2009;

"prescribed credential" means a verifiable credential other than SevisPass that is prescribed by regulation or recognised under the National Digital Identity and Trust Services Framework for issuance, holding, presentation or verification under this Act;

"public body" means "public body" as defined by the *Public Finances (Management) Act* 1995;

"public interest" means the interests of the people of Papua New Guinea in the security, integrity, availability, accountability and trustworthiness of the National Digital Trust Ecosystem, and includes public health, public safety, public welfare, economic

wellbeing, the protection of the rights of individuals and the proper administration of this Act, but is not limited to those matters;

"Recognised Verifiable Credential Issuer" means a person or entity recognised by or under this Act as authorised to issue verifiable credentials, including digital identity credentials, within the National Digital Trust Ecosystem, and includes SevisPass while so recognised;

"Regulations" means regulations made under this Act;

"resident" means a citizen of Papua New Guinea, a permanent resident, or a legally recognised foreign national eligible under this Act to enrol for SevisPass;

"Secure Digital Exchange or Interoperability Platform" means a platform approved by the Regulator for secure, consent-governed data exchange and interoperability within the National Digital Trust Ecosystem, and includes SevisDEx while so approved;

"serious cybersecurity incident" means a cybersecurity incident that has caused, or poses an imminent and significant risk of causing, harm to the confidentiality, integrity or availability of SevisPass, SevisWallet, SevisDEx, the Trust Registry or another critical system forming part of the National Digital Trust Ecosystem, including an incident involving unauthorised access, a data breach, denial of service, malicious software or compromise of cryptographic material, that is of a nature or scale prescribed by regulation or notified as such by the National Cyber Security Centre;

"SevisAdminPortal" means the administrative and governance platform approved under this Act for trust registry, credential issuance management, revocation management and related administrative functions;

"SevisDEx" means the secure government and business data exchange platform used within the National Digital Identity and Trust Services Framework for consent-governed data sharing and interoperability;

"SevisPass" means the verifiable credential established under this Act as the trust anchor of the National Digital Trust Ecosystem, within which a holder's primary biometric is enrolled and anchored for the purposes of deduplication, and to which other verifiable credentials issued under this Act may be linked; and does not constitute proof of citizenship or nationality;

"SevisWallet" means Papua New Guinea's official national digital wallet designated under this Act for the holding, management, storage, presentation and verification of SevisPass and prescribed verifiable credentials;

"Special Purpose Vehicle" or "SPV" means a body corporate established or designated for the special and limited purpose of implementing, operating or administering, as a neutral utility, the operational aspects of the National Digital Trust Ecosystem

necessary for the digital economy to thrive, and designated as the Implementation Authority under Section 32;

"selective disclosure" means the capability of a holder, through an approved digital wallet, to disclose only the minimum identity or credential attribute, proof, status or entitlement required for a lawful purpose without disclosing unnecessary personal data;

"Trust Registry" means the register maintained by or under the authority of the Regulator of authorised issuers, accredited partners, approved digital wallets, credential schemas, trust services and other matters prescribed under this Act;

"Trust Service" means an accredited digital service that enables secure, trusted and legally recognised digital interactions within the National Digital Trust Ecosystem, and includes, without limitation, digital identity services, digital identity authentication services, digital identity provision, identity proofing and assurance services, the issuance, exchange, presentation, verification, suspension and revocation of verifiable credentials, digital wallet services, secure interoperability and trusted data exchange services, digital payment trust services, electronic signatures, electronic seals, electronic timestamps, credential status and verification services, and any other trust service prescribed under this Act;

"verifiable credential" means a cryptographically signed, tamper-evident digital statement issued by a trusted issuer, held by a holder and capable of being presented to a verifier for authentication or verification;

"verifier" means a person, entity or system that requests, receives or verifies a verifiable credential or a presentation derived from it for the purpose of confirming identity, attributes, entitlements, status or authority.

5. APPLICATION

(1) This Act applies throughout Papua New Guinea.

(2) This Act binds the State.

(3) This Act applies to—

(a) SevisPass;

(b) SevisWallet;

(c) prescribed credentials;

(d) authorised issuers;

(e) accredited partners;

(f) approved digital wallets;

(g) verifiers subject to this Act; and

(h) any other person or entity prescribed by regulation.

(4) This Act applies subject to the Constitution and any other Constitutional Law.

6. RELATIONSHIP WITH OTHER LAWS

(1) This Act shall be read subject to the Constitution.

(2) Nothing in this Act affects the operation of—

(a) the *Citizenship Act* 1975;

(b) the *Migration Act* 1978;

(c) the *Passports Act* 1982;

(d) the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015;

(e) the *Civil and Identity Registration Act* 2024;

(f) the *Public Finances (Management) Act* 1995; or

(g) any other law prescribed by regulation,

except to the extent expressly provided by this Act or a consequential amendment made by this Act.

(3) Where another written law expressly requires physical production of a document, this Act does not displace that requirement unless that law is amended or the contrary intention appears.

PART II. — NATIONAL DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS SYSTEM

Division 1. — Establishment of SevisPass

7. ESTABLISHMENT OF SEVISPASS

(1) SevisPass is hereby established as a verifiable credential, and as the trust anchor of the National Digital Trust Ecosystem, within which a holder's primary biometric is enrolled and anchored for the purposes of deduplication.

(2) SevisPass shall be issued under this Act in accordance with the National Digital Identity and Trust Services Framework and any applicable regulations.

(3) SevisPass is the primary verifiable credential to which other prescribed credentials issued under this Act may be anchored or linked in accordance with this Act and the regulations.

8. NATURE AND EFFECT OF SEVISPASS

(1) SevisPass—

(a) is a verifiable credential issued under this Act as the trust anchor of the National Digital Trust Ecosystem;

(b) is digital by default;

(c) may be held and managed through SevisWallet or another approved digital wallet; and

(d) shall have the legal status conferred by this Act.

(2) SevisPass—

(a) does not constitute proof of citizenship or nationality;

(b) does not of itself constitute a passport, visa, travel document, licence, permit, entitlement or certificate unless another written law expressly provides otherwise; and

(c) shall not be used to infer citizenship, migration status or any other legal status beyond the credential attributes lawfully associated with it.

9. ELIGIBILITY FOR SEVISPASS

(1) Every resident is eligible to apply for SevisPass in accordance with this Act.

(2) Eligibility criteria, enrolment classes and supporting evidence requirements may be further prescribed by regulation.

(3) Eligibility provisions shall be administered consistently with the *Citizenship Act* 1975 and the *Migration Act* 1978.

10. ONE SEVISPASS FOR LIFE

(1) Subject to this Act, an individual shall be issued only one SevisPass for life.

(2) Re-issuance, replacement, restoration, update, correction, suspension and revocation of a SevisPass do not create a new identity record except as prescribed for fraud control, deduplication or system rectification.

11. CHARACTERISTICS OF SEVISPASS

(1) SevisPass shall have the following characteristics:

(a) a randomly generated non-intelligent identifier of twelve (12) digits containing no embedded personal information;

(b) cradle-to-grave validity, subject to lawful suspension, correction, revocation or update;

(c) capability for online and offline authentication, to the extent technically feasible;

(d) authentication functionality in accordance with approved technical standards; and

(e) such further characteristics as may be prescribed by regulation.

(2) SevisPass may be issued to a child in accordance with regulations that provide for demographic-only enrolment until the prescribed age for biometric collection is reached.

12. SEVISPASS LIFECYCLE

The lifecycle of SevisPass includes—

(a) registration and enrolment;

(b) verification, deduplication and issuance;

(c) holding, management, use, authentication and verification;

(d) correction, update, suspension, reactivation and revocation; and

(e) archival, retention and other end-of-lifecycle matters prescribed by regulation.

Division 2. — SevisWallet and Approved Digital Wallets

13. DESIGNATION OF SEVISWALLET

(1) SevisWallet is hereby designated as Papua New Guinea's official national digital wallet for the purposes of this Act.

(2) SevisWallet shall be used for the holding, management, storage, presentation and verification of SevisPass and prescribed credentials in accordance with this Act.

(3) SevisWallet shall support holder rights, selective disclosure, consent controls, audit history, interoperability and portability in accordance with this Act and the regulations.

14. APPROVED DIGITAL WALLETS

(1) The Regulator may approve additional digital wallets for use under this Act.

(2) A digital wallet shall not be approved unless the Regulator is satisfied that it—

(a) complies with the National Digital Identity and Trust Services Framework;

(b) preserves holder rights under this Act;

(c) supports interoperability with SevisWallet and SevisDEx;

(d) supports selective disclosure where technically feasible;

(e) provides adequate security, resilience, audit logging and incident response capability; and

(f) does not undermine SevisWallet's status as the official State-designated national digital wallet.

(3) Approval may be granted subject to conditions.

Division 3. — Verifiable credentials ecosystem

15. ESTABLISHMENT OF VERIFIABLE CREDENTIALS ECOSYSTEM

(1) There is established under this Act a national verifiable credentials ecosystem forming part of the National Digital Identity and Trust Services Framework.

(2) The ecosystem shall provide for the lawful issuance, holding, presentation, verification, suspension, revocation and legal recognition of verifiable credentials by—

(a) authorised issuers;

(b) accredited issuers;

(c) approved digital wallets;

(d) verifiers; and

(e) other trust service participants prescribed by regulation.

16. PRESCRIBED CREDENTIAL CATEGORIES

(1) Without limiting the generality of Section 16, the following categories of prescribed credentials may be issued, recognised, held, presented and verified under this Act—

(a) driver's licences;

(b) passports;

(c) visas;

(d) work permits;

(e) birth certificates;

(f) Grade 12 certificates;

(g) Tax Identification Number certificates;

(h) police clearance certificates;

(i) student identification credentials;

(j) teacher identification credentials;

(k) professional membership or licensing credentials;

(l) superannuation credentials; and

(m) any other category prescribed by regulation or recognised under the National Digital Identity and Trust Services Framework.

(2) The inclusion of a credential in Subsection (1) does not, of itself, amend or displace the enabling law governing that credential.

17. AUTHORISED ISSUERS

(1) A public body specified in the regulations or under another written law may be an authorised issuer for a credential category.

(2) An authorised issuer may issue a verifiable credential only within the scope of its statutory functions.

(3) An authorised issuer must ensure that the credential issued by it—

(a) is lawfully authorised;

(b) is accurate and current so far as reasonably practicable;

(c) conforms to the applicable credential schema; and

(d) is subject to lawful correction, update, suspension or revocation procedures.

18. ACCREDITED ISSUERS

(1) A private-sector entity shall not issue a verifiable credential under this Act unless it is accredited as an accredited issuer.

(2) The Regulator may accredit a private-sector entity as an accredited issuer subject to this Act and the regulations.

(3) Accreditation may be granted only if the entity satisfies eligibility, governance, technical, security, financial and compliance requirements prescribed by this Act or the regulations.

19. CREDENTIAL SCHEMAS

(1) The Regulator may approve or prescribe credential schemas for categories of verifiable credentials.

(2) A credential schema may specify—

(a) minimum and optional attributes;

(b) data quality requirements;

(c) encoding standards;

(d) validation rules;

(e) revocation and status-check requirements; and

(f) interoperability requirements.

20. LEGAL RECOGNITION OF VERIFIABLE CREDENTIALS

(1) A verifiable credential issued under this Act has legal recognition for any purpose for which the underlying document, certificate, licence, permit, entitlement, status or authority would otherwise be recognised, unless another written law expressly requires otherwise.

(2) An electronic presentation of a verifiable credential under this Act shall not be denied legal effect merely because it is in digital form.

(3) A verifier shall not unreasonably refuse to accept a verifiable credential issued under this Act in lieu of the physical document it represents, unless—

(a) another written law expressly requires production of the physical document;

(b) the verifier has reasonable grounds to believe that the credential is invalid, suspended, revoked, expired, technically unverifiable, unlawfully presented or irrelevant to the transaction; or

(c) the transaction falls within a class prescribed by regulation as requiring additional evidence.

21. PRESENTATION AND VERIFICATION

(1) A holder may present a verifiable credential through SevisWallet or another approved digital wallet.

(2) A verifier shall—

(a) request only the minimum attributes or proof reasonably necessary for the stated lawful purpose;

(b) use selective disclosure where available and sufficient;

(c) comply with purpose limitation and data minimisation requirements; and

(d) not retain data beyond what is lawful and reasonably necessary.

22. SUSPENSION AND REVOCATION OF CREDENTIALS

(1) A SevisPass or prescribed credential may be suspended or revoked only—

(a) on grounds prescribed by this Act or the regulations; and

(b) in accordance with natural justice.

(2) Except in urgent circumstances prescribed by regulation, the affected holder shall be given—

(a) prior notice;

(b) reasons;

(c) an opportunity to respond; and

(d) notice of the right to review or appeal.

(3) Emergency temporary suspension may be effected without prior notice only where strictly necessary for fraud prevention, public safety, cybersecurity or the integrity of the system, and reasons shall be given as soon as practicable thereafter.

Division 4. — Mandatory Acceptance, Interoperability and Sovereign Infrastructure

23. MANDATORY ACCEPTANCE

(1) Public bodies shall, within 12 months after commencement of the relevant provision, accept SevisPass and applicable prescribed credentials for identity verification, credential validation and digital service access, subject to reasonable alternative channels for essential government services.

(2) Financial institutions, superannuation funds, payment service providers and other entities regulated for AML/CTF or by the Bank of Papua New Guinea shall, within 18 months after commencement of the relevant provision, accept SevisPass and applicable prescribed credentials for eKYC, customer due diligence, onboarding and attribute verification, subject always to their continuing legal obligations for customer risk assessment, transaction monitoring and sanctions screening.

(3) Telecommunications operators, educational institutions, transport authorities, professional bodies, utilities and other prescribed sectors shall comply within 24 to 36 months after commencement, as prescribed by regulation or sectoral instruction consistent with this Act.

(4) A sectoral regulator may issue implementing instructions in coordination with the Regulator but shall not narrow the substantive acceptance obligation established by this Act.

24. CROSS-BORDER RECOGNITION AND INTEROPERABILITY

(1) The Minister may, on advice of the Regulator and after consultation with relevant authorities, approve arrangements for cross-border recognition, verification and interoperability of SevisPass, SevisWallet and prescribed credentials.

(2) An arrangement under Subsection (1) shall not take effect unless the Minister is satisfied that it preserves—

(a) constitutional protections;

(b) privacy and consent requirements;

(c) cybersecurity and trust standards; and

(d) Papua New Guinea's sovereign control over core trust infrastructure.

24A. Foreign participation restrictions.

(1) In this section, foreign State-linked entity means an entity that is—

(a) owned or controlled, directly or indirectly, by a foreign government, foreign State instrumentality or foreign sovereign wealth fund; or

(b) subject to direction or control by a foreign government, whether through ownership, contract, law or otherwise.

(2) A foreign State-linked entity shall not be designated as the Implementation Authority.

(3) A change in ownership or control of the Implementation Authority that would result in a foreign person or foreign entity, alone or together with associates, holding a beneficial interest of 15% or more in the Implementation Authority shall not take effect without the prior written approval of the National Executive Council, on the advice of the Minister, following consultation with the Regulator.

(4) The Implementation Authority shall notify the Regulator within 14 days of becoming aware of any proposed change of ownership or control, including any transaction that would result in a change in the identity of persons who hold significant influence over the Implementation Authority.

(5) The Regulator may, where it is satisfied that a change of ownership or control poses a risk to the State's sovereign ownership or ultimate control of sovereign trust infrastructure, recommend to the Minister that—

(a) approval be refused or made subject to conditions; or

(b) revocation of the designation be considered under Section 38.

(6) A transaction entered into in contravention of this section is void to the extent of the contravention.

24B. Exercise of step-in rights procedure.

(1) The State's step-in rights under Section 37 may be activated by the National Executive Council by decision published in the National Gazette, on the advice of the Minister, where the NEC is satisfied that one or more of the triggering circumstances in Section 37(1) exists.

(2) Upon publication of a step-in decision, the Implementation Authority shall immediately—

(a) grant the State or its designated agent full access to all systems, data, credentials, source code, cryptographic materials and facilities constituting or supporting sovereign trust infrastructure;

(b) cooperate fully with the State or its designated agent in the orderly assumption of operational control; and

(c) cease any action that would impair, diminish or complicate the State's exercise of control.

(3) A step-in period shall not exceed 12 months, after which the National Executive Council shall either—

(a) restore the Implementation Authority to its functions, with or without conditions; or

(b) commence revocation under Section 38 and designate a successor under Section 37(2).

(4) Officers, employees and agents of the State acting in good faith in the exercise of step-in rights are not personally liable for any act done or omitted in the reasonable exercise of those rights.

(5) The Implementation Authority is not entitled to compensation for loss of revenue or commercial opportunity during a step-in period, but may claim reasonable reimbursement for documented costs directly and necessarily incurred in facilitating the step-in.

25. STATE OWNERSHIP AND SOVEREIGN CONTROL

(1) The State retains sovereign ownership and ultimate control over—

(a) SevisPass;

(b) SevisWallet;

(c) SevisDEx;

(d) the National Digital Identity and Trust Services Framework;

(e) the Trust Registry;

(f) public cryptographic trust anchors;

(g) credential schemas designated as sovereign trust infrastructure; and

(h) any other core digital public infrastructure designated by regulation.

(2) No contract, licence, concession, public-private partnership, outsourcing arrangement, shareholding arrangement or other instrument shall transfer ownership or ultimate control of sovereign trust infrastructure away from the State.

(3) Intellectual property in software, source code, application programming interfaces, cryptographic libraries, credential schemas, system architecture, technical documentation and related materials that are created specifically for the purposes of this Act or the National Digital Identity and Trust Services Framework, whether created by the Implementation Authority, by the State, or by a contractor or subcontractor engaged for those purposes, shall:

(a) where created by or on behalf of the State, vest in the State from the time of creation; and

(b) where created by or on behalf of the Implementation Authority using funding, infrastructure or resources of the State or the Digital Identity Sustainability Fund, vest in the State upon the termination, expiry or revocation of the Implementation Authority's designation, without further act, instrument or consideration.

(3A) During the period of designation, the Implementation Authority holds a non-exclusive, royalty-free licence to use intellectual property owned by the State under Subsection (3) solely for the purposes of its functions under this Act.

(3B) The Implementation Authority shall not, without the prior written approval of the Minister—

(a) assign, sublicence, mortgage, charge or otherwise encumber intellectual property in sovereign trust infrastructure;

(b) incorporate such intellectual property into a product or service offered commercially outside the National Digital Identity and Trust Services Framework; or

(c) allow a third party to assert rights over such intellectual property that would limit the State's full ownership following revocation or termination of the designation.

(3C) The Implementation Authority shall maintain a current source code and system documentation repository and shall, at intervals prescribed by the Regulator and on request, deposit a complete copy of all software and technical materials in escrow with a designated State custodian approved by the Regulator.

(4) The root cryptographic trust anchors, root certificate authority private keys, master signing keys and hardware security module credentials for sovereign trust infrastructure shall be—

(a) held in a secure facility approved by the Regulator and physically located within Papua New Guinea; and

(b) held under an arrangement that gives the State, acting through the Regulator, immediate and unrestricted access upon—

(i) the exercise of step-in rights under Section 37; or

(ii) the revocation or termination of the Implementation Authority's designation under Section 38.

(4A) The Implementation Authority shall maintain a cryptographic key escrow arrangement approved by the Regulator. Key material held in escrow shall be—

(a) protected against unauthorised access by technical and physical security measures prescribed by the Regulator;

(b) subject to independent verification by the Regulator at intervals not exceeding 12 months; and

(c) transferred to the State or to a designated successor authority without condition, delay or cost upon the activation of step-in rights or the revocation or termination of designation.

(4B) Key ceremonies, key generation, key rotation and key lifecycle management shall be conducted in accordance with procedures prescribed by the Regulator, and the Implementation Authority shall permit a representative of the Regulator to observe any key ceremony upon request.

(4C) A contravention of this subsection by the Implementation Authority is a ground for revocation of designation under Section 38.

(5) Subject to Subsection (5A), personal data, biometric data, credential data and audit logs collected or generated under this Act shall be stored on infrastructure physically located within Papua New Guinea.

(5A) Processing of data referred to in Subsection (5), other than biometric raw data and root cryptographic key material, which shall not be stored or processed offshore under any circumstances, may occur through offshore infrastructure only where—

(a) the Minister has, by notice in the National Gazette, approved the offshore facility and jurisdiction as meeting equivalent legal and security protections;

(b) the data remains encrypted and subject to Papua New Guinea's legal jurisdiction throughout transit and processing;

(c) the offshore facility is contractually prohibited from disclosing any data to a foreign government, authority or intelligence entity without the prior written consent of the Regulator; and

(d) the arrangement is reviewed by the Regulator at intervals not exceeding two years, and the Minister may revoke approval if the Regulator is no longer satisfied that the conditions in paragraphs (a) to (c) are met.

(5B) The Implementation Authority shall—

(a) notify the Regulator of all data processing arrangements, including cloud service providers, subcontractors and cross-border data transfers; and

(b) not enter into any new data processing arrangement involving offshore infrastructure without the prior written approval of the Regulator.

26. SUSTAINABILITY AND FEES

(1) The ecosystem established under this Act may be supported by a regulated revenue and sustainability framework.

(2) Fees may be prescribed for—

(a) verification services;

(b) accreditation;

(c) platform participation;

(d) institutional integration;

(e) trust services;

(f) payment-rail integration; and

(g) other commercial or institutional services prescribed by regulation.

(3) Fees shall be transparent, proportionate and non-discriminatory among similarly situated participants.

(4) No resident shall be charged for the basic functions of receiving, holding, managing, storing or presenting his own SevisPass or prescribed credentials through SevisWallet.

(5) There is hereby established a fund to be known as the Digital Identity Sustainability Fund (the *Fund*).

(5A) The Fund is established for the purposes of ensuring the long-term financial sustainability, resilience, inclusion and development of the National Digital Trust Ecosystem established under this Act.

(5B) The Fund shall consist of—

(a) fees collected under Subsection (2);

(b) platform participation levies prescribed by regulation;

(c) commercial service revenues attributed to the Fund under the Implementation Authority's designation instrument;

(d) appropriations by Parliament for ecosystem development;

(e) grants, donations or contributions from development partners, international organisations or the private sector; and

(f) income earned on the Fund's authorised investments.

(5C) The Fund shall be managed by the Regulator in trust for the State, subject to direction by the Minister, and shall be applied only to—

(a) the operational and capital costs of the Implementation Authority, as certified by the Regulator as reasonable and consistent with the designation instrument;

(b) inclusion and accessibility initiatives, including digital enrolment for persons in remote areas, persons with disabilities and other vulnerable persons;

(c) cybersecurity capability, infrastructure investment and resilience for sovereign trust infrastructure;

(d) research, standards development and international and regional engagement in digital identity; and

(e) the costs reasonably incurred by the Regulator in administering this Act.

(5D) The Fund is subject to audit by the Auditor-General of Papua New Guinea and to annual reporting to the National Parliament as part of the annual report required under Section 32.

(5E) The Fund is not available for appropriation to general government purposes except by express Act of the National Parliament.

(6) The Implementation Authority may, with the approval of the Regulator and the written consent of the Minister, offer the following categories of commercial services on a fee-for-service basis within the National Digital Identity and Trust Services Framework—

(a) enhanced identity assurance services for high-value or high-risk transactions at assurance levels above the standard level prescribed by the Regulator;

(b) identity-as-a-service for regulated financial institutions, insurers, superannuation funds and other prescribed entities;

(c) bulk and batch verification services and application programming interface access for institutional users;

(d) consent-governed attribute data-sharing services through SevisDEx for commercial purposes authorised by credential holders;

(e) technology licensing or technical assistance arrangements with other Pacific Island states or regional bodies, on terms approved by the National Executive Council;

(f) integration services for public bodies beyond the mandatory acceptance obligations established by Section 23; and

(g) such other commercial services as the Minister approves by notice in the National Gazette, having regard to the advice of the Regulator.

(6A) Every accredited partner operating within the National Digital Identity and Trust Services Framework shall pay a platform participation levy to the Fund, calculated by reference to the volume of verifications, credential issuances or data-sharing transactions conducted by that partner in the preceding year. The Regulator shall prescribe the levy rate, which shall be—

(a) proportionate to usage;

(b) non-discriminatory among accredited partners in the same category; and

(c) reviewed annually.

(6B) Fees charged for commercial services under Subsection (6) shall not be applied to reduce the State's funding obligations for basic public identity services, and no commercial arrangement shall result in a resident being charged for the functions protected under Subsection (4).

PART III — REGULATOR

27. DESIGNATION OF REGULATOR

(1) The entity for the time being responsible for the regulation of information and communications technology and the digital economy is designated as the Regulator for the purposes of this Act. (2) Unless and until another entity is designated by or under the *National Information and Communications Technology Act* 2009 or a Gazette notice made under that Act, the Regulator is the National Information and Communications Technology Authority.

28. FUNCTIONS OF REGULATOR

The functions of the Regulator are—

(a) to develop, administer and enforce the National Digital Identity and Trust Services Framework;

(b) to approve standards, credential schemas, trust services and interoperability requirements;

(c) to accredit, supervise, suspend and revoke accredited partners;

(d) to approve and supervise approved digital wallets;

(e) to maintain or cause to be maintained the Trust Registry;

(f) to monitor compliance with this Act;

(g) to conduct audits and inspections;

(h) to investigate contraventions;

(i) to issue directions and administrative penalties in accordance with this Act;

(j) to advise the Minister on commencement sequencing, sectoral transition and cross-border arrangements;

(k) to promote holder rights and public awareness; and

(l) to perform any other function conferred by this Act or another law.

29. POWERS OF REGULATOR

The Regulator has power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Act, including power to—

(a) issue standards, codes, rules and technical requirements consistent with this Act and the regulations;

(b) require information, records and reports;

(c) enter into lawful coordination arrangements with sectoral regulators and public bodies;

(d) impose conditions on approvals and accreditations;

(e) establish registers and digital assurance mechanisms; and

(f) apply to the National Court for an injunction under this Act.

30. LIMITATION CONCERNING AML/CTF FUNCTIONS

Nothing in this Act authorises the Regulator to require SevisPass, SevisWallet or the National Digital Identity and Trust Services Framework to perform customer risk ratings, transaction monitoring or sanctions screening, which remain the legal responsibility of financial institutions and other regulated entities under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 and other applicable laws.

31. TECHNICAL STANDARDS AND ADVISORY COMMITTEE

(1) The Regulator shall establish a Technical Standards and Advisory Committee.

(2) The Committee shall include representatives of—

(a) relevant government agencies;

(b) the private sector;

(c) civil society;

(d) technical experts; and

(e) such other stakeholders as the Regulator considers appropriate.

(3) The functions, procedures and terms of reference of the Committee may be prescribed by regulation or determined by the Regulator consistently with this Act.

32. ANNUAL REPORT

The Regulator shall submit to the Minister and to the National Parliament an annual report on the operation, performance, compliance, security and development of the National Digital Trust Ecosystem established under this Act.

PART IV — NATIONAL DIGITAL IDENTITY AND TRUST SERVICES FRAMEWORK IMPLEMENTATION AUTHORITY

33. DESIGNATION OF IMPLEMENTATION AUTHORITY

(1) Unless the National Executive Council otherwise directs on the advice of the Minister by decision published in the National Gazette, the Minister may, by notice in the National Gazette, designate an entity as the National Digital Identity and Trust Services Framework Implementation Authority. In particular, the Minister may designate a Special Purpose Vehicle to operate as a neutral utility for the specific purpose of providing the infrastructure necessary for the digital economy to thrive.

(2) The designation instrument shall identify—

(a) the name of the entity;

(b) the functions designated to it;

(c) the date on which the designation takes effect;

(d) the categories of commercial services the Implementation Authority is authorised to offer under Section 26(6);

(e) the revenue allocation arrangement, including the proportion of fee revenue to be retained by the Implementation Authority for operational costs and the proportion to be remitted to the Digital Identity Sustainability Fund;

(f) the Implementation Authority's obligations in relation to intellectual property under Section 25(3), cryptographic key custody under Section 25(4) and data residency under Section 25(5);

(g) reporting obligations on revenue, expenditure, system performance and material security incidents;

(h) any conditions of designation; and

(i) any transition or continuity arrangements.

(3) The designated entity is subject to this Act notwithstanding anything in its constitution or constituting instrument.

34. CRITERIA FOR DESIGNATION

Following a direction of the National Executive Council upon the advice of the Minister, the National Executive Council, acting through the Minister, shall not designate an entity under Section 33 unless satisfied that the entity—

(a) has the technical, operational and financial capacity to discharge the designated functions;

(b) can maintain continuity, resilience and cybersecurity for core services;

(c) can operate consistently with State ownership and sovereign control requirements;

(d) can comply with public finance, procurement and accountability laws; and

(e) satisfies any additional criteria prescribed by regulation; and

(f) has a governance structure that preserves State control over sovereign trust infrastructure through a golden share or equivalent mechanism consistent with Section 36, and can operate with the neutrality required of a utility providing infrastructure for the digital economy.

35. FUNCTIONS OF IMPLEMENTATION AUTHORITY

The functions of the Implementation Authority are—

(a) to design, deploy, operate and maintain the core operational components of the ecosystem assigned to it;

(b) to operate or support SevisPass, SevisWallet, SevisDEx, SevisPay, SevisAdminPortal and related systems as lawfully designated;

(c) to support interoperability, credential lifecycle management and platform continuity;

(d) to maintain operational audit logs and incident response arrangements;

(e) to provide reports and information to the Regulator and the Minister; and

(f) to perform other functions conferred by this Act, the regulations or the notice of designation.

(g) to develop and offer, within the National Digital Identity and Trust Services Framework and in accordance with Section 26(6) and any written approval of the Minister, commercial services that generate sustainable revenue for the Digital Identity Sustainability Fund and support the long-term viability of the ecosystem.

36. GOVERNANCE REQUIREMENTS

(1) The following governance requirements apply to the Implementation Authority and prevail over any inconsistent constitution, charter, constituting instrument or contract:

(a) the board shall include the classes of representation prescribed by regulation, including public-sector and stakeholder representation;

(b) the Implementation Authority shall publish an annual report covering system performance, material security incidents, financial statements and compliance;

(c) risk management protocols aligned with the current applicable national policy and strategy shall be maintained including with the National Security Policy 2024-2029, the National Cybersecurity Policy 2021 and National Cybersecurity Strategy 2024; and

(d) contracts entered into by the Implementation Authority involving sovereign trust infrastructure shall—

(i) comply with public procurement and public finance requirements;

(ii) not transfer sovereign ownership or ultimate control of sovereign trust infrastructure away from the State;

(iii) be disclosed to the Regulator before execution;

(iv) contain a termination-for-convenience clause exercisable by the Implementation Authority on the written direction of the Minister, without liability to the vendor beyond reasonable notice and documented direct costs; and

(v) not contain any change-of-control or insolvency provision that would give a technology vendor, financier or third party rights over sovereign trust infrastructure that could be asserted against the State.

(e) sovereign trust infrastructure, including cryptographic key material, the Trust Registry and core biometric deduplication systems, shall be ring-fenced in the accounts, security architecture and asset register of the Implementation Authority from its other assets, business lines and creditors, so that it is not available to satisfy the debts or liabilities of the Implementation Authority or, where applicable, of its owners;

(f) the instrument of designation or constituting instrument shall reserve to the State a golden share or equivalent mechanism sufficient to preserve State control over sovereign trust infrastructure, irrespective of the Implementation Authority's ownership or capital structure;

(g) the Implementation Authority shall provide access to its core services on a non-discriminatory, reasonable and transparent basis to authorised issuers, accredited

partners, verifiers and other Ecosystem participants, and any fee, charge or tariff levied by the Implementation Authority for its core services is subject to the prior approval of the Regulator.

(2) Additional governance requirements may be prescribed by regulation or included in the designation notice.

37. CONTINUITY AND STEP-IN POWERS

(1) The State shall have step-in rights, to be exercised in accordance with law and any applicable instrument, in matters involving—

(a) national security;

(b) continuity of service;

(c) material system failure;

(d) serious cybersecurity incident; or

(e) protection of the public interest.

(2) Where the designation of an Implementation Authority is revoked or has not less than a term of twelve (12) months remaining, the National Executive Council may, on the advice of the Minister by decision published in the National Gazette—

(a) designate a successor entity; or

(b) vest functions temporarily in the Department or other designated public body by notice in the National Gazette,

so as to preserve continuity of service and holder access to credentials.

38. REVOCATION OF DESIGNATION

(1) The National Executive Council on the advice of the Minister, may revoke a designation by notice in the National Gazette if the designated entity—

(a) ceases to satisfy the criteria for designation;

(b) commits a serious or repeated contravention of this Act;

(c) becomes incapable of discharging its functions; or

(d) otherwise fails to comply with a condition of designation.

(2) Before revoking a designation, the Minister shall give notice and an opportunity to respond, unless urgent public interest requires immediate action.

PART V — ACCREDITED PARTNERS

39. CATEGORIES OF ACCREDITED PARTNERS

The following categories of accredited partners may be recognised under this Act—

(a) accredited issuers;

(b) accredited verifiers;

(c) approved digital wallet providers;

(d) enrolment agents or enrolment partners;

(e) trust service providers;

(f) technical integration providers; and

(g) any other class prescribed by regulation.

40. REQUIREMENT FOR ACCREDITATION

A person or entity shall not operate as an accredited partner under this Act unless accredited or approved in accordance with this Act.

41. APPLICATION FOR ACCREDITATION

(1) An application for accreditation shall be made to the Regulator in the prescribed form and accompanied by the prescribed information and fee, if any.

(2) The applicant must demonstrate compliance with requirements concerning governance, security, technical capability, financial capacity, privacy, data protection and legal compliance including additional requirements as prescribed by regulation.

42. GRANT, CONDITIONS AND DURATION OF ACCREDITATION

(1) The Regulator may grant or refuse accreditation.

(2) Accreditation may be granted subject to terms and conditions.

(3) Accreditation remains in force for the period prescribed or until suspended, revoked, surrendered or expired.

43. OBLIGATIONS OF ACCREDITED PARTNERS

An accredited partner shall—

(a) comply with this Act, the regulations and any applicable standards;

(b) protect privacy and personal data;

(c) maintain cybersecurity, resilience and audit logging;

(d) cooperate with lawful inspections and audits;

(e) notify the Regulator of material incidents, breaches or changes of control within the prescribed time; and

(f) comply with any conditions of accreditation.

44. SUSPENSION AND REVOCATION OF ACCREDITATION

(1) The Regulator may suspend or revoke an accreditation on grounds prescribed by this Act or the regulations.

(2) Except where urgent action is necessary, suspension or revocation shall not occur unless the accredited partner has been given—

(a) notice of the proposed action;

(b) reasons; and

(c) an opportunity to respond.

PART VI — RIGHTS OF CREDENTIAL HOLDERS

45. RIGHT TO ENROL

Every eligible resident has the right to apply for SevisPass and shall not be unreasonably refused enrolment.

46. RIGHT OF ACCESS

A holder has the right to access his SevisPass profile, credential data and related records in the manner prescribed.

47. RIGHT OF CORRECTION

A holder may apply, through prescribed channels, for correction of inaccurate or incomplete data relating to SevisPass or another credential issued under this Act.

48. RIGHT TO CONSENT-BASED SHARING

(1) Except where disclosure is required or authorised by written law, a holder's credential data shall not be disclosed from SevisWallet or another approved digital wallet without the holder's explicit, informed and contemporaneous consent.

(2) Consent shall be capable of being evidenced, managed and revoked in the prescribed manner.

49. RIGHT TO REVOKE CONSENT

A holder may revoke consent previously given for access, disclosure or sharing of credential data, subject to any lawful retention, audit or record-keeping obligation.

50. RIGHT TO NOTIFICATION

Subject to lawful restriction, a holder is entitled to be notified when his credential data is accessed, presented, shared or verified.

51. RIGHT TO DISCLOSURE HISTORY

A holder is entitled to access a record of disclosures, presentations and verifications made from his approved digital wallet, except to the extent lawfully restricted for law enforcement, national security or another prescribed reason.

52. RIGHT TO DELETION OR REMOVAL FROM WALLET

A holder may request deletion or removal of a credential from an approved digital wallet, subject to the lawful retention obligations of the issuer in respect of the underlying record.

53. RIGHT TO PORTABILITY

A holder may export, transfer or re-establish his verifiable credentials in another approved digital wallet or successor wallet, subject to lawful security and anti-fraud requirements.

54. RIGHT TO CONTINUITY

A holder's access to credentials shall not be unreasonably interrupted by a change in operator, implementation authority, technology vendor or approved wallet provider.

55. RIGHT TO REDRESS

A holder whose rights under this Act are affected may—

(a) lodge a complaint with the Regulator;

(b) seek corrective action;

(c) seek review in accordance with this Act; and

(d) appeal to the National Court.

56. SPECIAL PROVISIONS FOR VULNERABLE PERSONS

The Regulator, the Implementation Authority, issuers and wallet providers shall make reasonable accommodations for persons with disabilities, elderly persons, children, persons in remote areas and other vulnerable persons prescribed by regulation.

PART VII — DATA PROTECTION AND PRIVACY

57. PRIVACY BY DESIGN

Every entity operating under this Act shall implement privacy by design in systems, processes, products and services used for digital identity and verifiable credentials.

58. SELECTIVE DISCLOSURE

Every approved digital wallet, including SevisWallet, shall support selective disclosure where technically feasible.

59. RELATIONSHIP WITH DATA GOVERNANCE, PRIVACY AND DATA PROTECTION ACT

(1) The *Data Governance, Privacy and Data Protection Act* 2026 governs personal data, data governance, data protection, privacy rights, data processing obligations, consent requirements, data sharing, data security, data breach management and data subject rights in respect of personal data processed within the National Digital Trust Ecosystem.

(2) This Act does not duplicate a matter referred to in Subsection (1), and a requirement of the Data Governance, Privacy and Data Protection Act 2026 applies concurrently with this Act to a person or entity operating within the National Digital Trust Ecosystem.

(3) The Regulator and the regulator designated under the *Data Governance, Privacy and Data Protection Act* 2026 shall cooperate and coordinate in the administration and enforcement of the respective Acts, including through information-sharing arrangements and joint guidance where appropriate.

(4) Nothing in this Act limits the application of the *Data Governance, Privacy and Data Protection Act* 2026 to personal data processed within the National Digital Trust Ecosystem.

PART VIII — ENFORCEMENT, OFFENCES AND APPEALS

Division 1. — Enforcement Powers

60. AUDITS AND INSPECTIONS

The Regulator may conduct audits and inspections of authorised issuers, accredited partners, approved digital wallets, verifiers and other ecosystem participants for the purpose of monitoring compliance with this Act.

61. COMPLIANCE DIRECTIONS

(1) Where the Regulator reasonably believes that a person has contravened or is contravening this Act, it may issue a written compliance direction.

(2) A person to whom a compliance direction is given shall comply with it within the time specified, unless review or appeal is commenced and a stay is granted.

62. INFORMATION-GATHERING POWERS

The Regulator may require a person subject to this Act to produce information, records or documents reasonably required for administration or enforcement of this Act.

63. ADMINISTRATIVE PENALTIES

(1) The Regulator may impose an administrative penalty for a prescribed contravention of this Act.

(2) An administrative penalty shall not be imposed unless—

(a) notice of the proposed penalty is given;

(b) the person is afforded an opportunity to respond; and

(c) reasons for the decision are given.

(3) The amount of an administrative penalty shall be [PGK amount or formula to be settled following State Solicitor and DJAG advice].

64. INJUNCTIONS

The Regulator may apply to the National Court for an injunction to restrain an actual or apprehended contravention of this Act.

Division 2. — Offences

65. FRAUDULENT ENROLMENT OR USE

A person who fraudulently enrols for, obtains, uses, presents or causes to be issued a SevisPass or other credential under this Act commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 50,000 to PGK 100,000] or imprisonment for a term not exceeding [term to be settled], or both; and

(b) in the case of a body corporate — a fine not exceeding [PGK 250,000 to PGK 500,000].

66. UNLAWFUL COLLECTION OR USE OF BIOMETRIC DATA

A person who unlawfully collects, accesses, discloses, sells, transfers or uses biometric data obtained under this Act commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 50,000] or imprisonment for a term not exceeding [term to be settled], or both; and

(b) in the case of a body corporate — a fine not exceeding [PGK 500,000].

67. UNAUTHORISED ACCESS TO SEVISDEX, TRUST REGISTRY OR RELATED SYSTEMS

A person who, without lawful authority, accesses, interferes with, alters, impairs, disrupts or attempts to access or interfere with SevisDEx, the Trust Registry, SevisWallet, SevisAdminPortal or another core system under this Act commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 20,000 to PGK 50,000] or imprisonment for a term not exceeding [term to be settled], or both; and

(b) in the case of a body corporate — a fine not exceeding [PGK 100,000 to PGK 500,000].

68. OPERATING WITHOUT ACCREDITATION OR APPROVAL

A person who operates as an accredited partner, accredited issuer, approved wallet provider or other regulated participant under this Act without the required accreditation or approval commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 10,000]; and

(b) in the case of a body corporate — a fine not exceeding [PGK 100,000].

69. FAILURE TO COMPLY WITH DIRECTION

A person who, without reasonable excuse, fails to comply with a lawful direction of the Regulator commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 5,000]; and

(b) in the case of a body corporate — a fine not exceeding [PGK 50,000].

70. FAILURE TO NOTIFY NOTIFIABLE DATA BREACH

A person or entity required to notify a data breach under this Act who, without reasonable excuse, fails to do so within the prescribed period commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 5,000]; and

(b) in the case of a body corporate — a fine not exceeding [PGK 50,000].

71. CONTRAVENTION OF CONSENT REQUIREMENTS

A person who knowingly causes credential data to be disclosed from an approved digital wallet without the consent required by this Act, and without lawful authority, commits an offence.

Penalty:

(a) in the case of an individual — a fine not exceeding [PGK 5,000 to PGK 20,000]; and

(b) in the case of a body corporate — a fine not exceeding [PGK 50,000 to PGK 200,000].

72. UNLAWFUL REFUSAL TO ACCEPT PRESCRIBED CREDENTIALS

(1) A person or entity subject to a mandatory acceptance obligation under this Act that unlawfully or unreasonably refuses to accept SevisPass or a prescribed credential commits a contravention.

(2) A contravention under this section may be dealt with by—

(a) compliance direction;

(b) administrative penalty;

(c) suspension or regulatory sanction; or

(d) such other consequence as may be prescribed.

Division 3. — Liability and Appeals

73. ALLOCATION OF LIABILITY

(1) An authorised issuer or accredited issuer is responsible for the lawful authority, accuracy, validity, status, suspension, revocation and timely updating of credentials issued by it.

(2) A verifier is responsible for—

(a) making lawful and proportionate requests;

(b) obtaining consent where required;

(c) complying with purpose limitation and data minimisation; and

(d) securely handling credential data within its control.

(3) An approved digital wallet provider and the Implementation Authority are responsible for operational availability, integrity of wallet services, presentation functionality, audit logging and incident response within their control.

(4) The Regulator is responsible for accreditation, standards, supervision, enforcement and maintenance of the Trust Registry in accordance with this Act.

(5) A holder is not liable for system errors, issuer errors, verifier misuse, operator failures or unauthorised third-party access unless the holder knowingly commits fraud, impersonation, misrepresentation or other unlawful conduct.

74. REVIEW BY REGULATOR

A person aggrieved by a decision of an officer or delegate under this Act may apply for internal review in the prescribed manner.

75. APPEAL TO NATIONAL COURT

(1) A person aggrieved by—

(a) a decision to refuse, suspend or revoke accreditation;

(b) a decision to suspend or revoke a credential;

(c) a decision to impose an administrative penalty;

(d) a compliance direction; or

(e) any other prescribed decision,

may appeal to the National Court within [30] days after notice of the decision or within such further time as the Court allows.

(2) The commencement of an appeal does not operate as a stay unless the National Court otherwise orders.

PART IX — MISCELLANEOUS, TRANSITIONAL AND SAVINGS

76. REGULATIONS

The Head of State, acting on advice, may make regulations, not inconsistent with this Act, prescribing matters required or permitted by this Act to be prescribed or necessary or convenient to be prescribed for carrying out or giving effect to this Act.

77. MATTERS THAT MAY BE PRESCRIBED BY REGULATION

Without limiting Section 77, regulations may provide for—

(a) technical standards for biometric and demographic data capture, exchange and authentication;

(b) accreditation criteria and procedures;

(c) data retention and deletion periods;

(d) grievance handling procedures and timeframes;

(e) fee schedules and revenue arrangements;

(f) form and authentication modalities of SevisPass;

(g) trust registry rules;

(h) wallet standards and approved trust services;

(i) selective disclosure, consent and audit requirements;

(j) staged mandatory acceptance;

(k) cross-border interoperability arrangements;

(l) electronic signatures, electronic seals, electronic timestamps and digital payment trust services; and

(m) any other matter necessary for the effective administration of this Act.

78. NATIONAL EXECUTIVE COUNCIL OVERSIGHT

Regulations made under this Act shall be laid before the National Executive Council for approval and signed by the Head of State, acting on advice.

79. TRANSITIONAL VALIDATION OF EXISTING PILOTS AND ISSUANCES

(1) Any government digital identity pilot programme, provisional SevisPass issuance, trial credential, technical arrangement or related implementation undertaken before the commencement of this section may, by regulation or ministerial notice consistent with law, be validated for the purposes of this Act.

(2) A validation under Subsection (1) shall not operate to deprive a person of a right, review or remedy under this Act.

80. CONTINUATION OF CERTAIN EXISTING INSTRUMENTS

(1) Regulations, rules, directions, memoranda of understanding, operating agreements or technical arrangements made under the *National Information and Communication Technology Act* 2009 or the *Digital Government Act* 2022 that relate to digital identity and are not inconsistent with this Act continue in force, according to their terms, until repealed, replaced or superseded.

(2) A person operating under an arrangement continued by this section shall comply with any accreditation or approval requirement under this Act within the transitional period prescribed by regulation.

81. MINISTER TO DESIGNATE IMPLEMENTATION AUTHORITY

The Minister shall designate an Implementation Authority within [12] months after the commencement of Part IV, unless the National Executive Council otherwise directs on the advice of the Minister by decision published in the National Gazette.

82. SAVINGS CONCERNING CITIZENSHIP AND NATIONALITY

Nothing in this Act shall be taken to mean that SevisPass constitutes proof of citizenship or nationality for any purpose under the *Citizenship Act* 1975 or any other law.

83. SAVINGS CONCERNING PASSPORTS AND TRAVEL

A passport credential or other travel-related credential held in SevisWallet is not itself a travel document unless recognised as such under the *Passports Act* 1982, the *Migration Act* 1978 or another applicable law.

84. SAVINGS CONCERNING AML/CTF OBLIGATIONS

Nothing in this Act limits or affects the rights, duties or obligations of financial institutions or other regulated entities under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 with respect to customer risk assessment, transaction monitoring, sanctions screening or related compliance.

85. SAVINGS CONCERNING CONSTITUTIONAL OVERSIGHT

Nothing in this Act affects the jurisdiction of the Ombudsman Commission, the courts or any other body exercising oversight functions under the Constitution or another law.

86. PRIVACY SAVINGS

The right of residents of Papua New Guinea under Section 49 of the Constitution are limited by this Act only to the extent expressly provided by this Act, and nothing in this Act authorises any further limitation.

87. POST-LEGISLATIVE SCRUTINY

(1) The Minister shall, within 3 years after the date on which the last of the provisions of this Act comes into operation, cause a comprehensive review of the operation and effectiveness of this Act to be conducted.

(2) The review must assess—

(a) whether this Act has achieved its stated objectives;

(b) the impact of this Act on the rights of credential holders, including vulnerable persons;

(c) the adequacy of the privacy and data protection provisions in Part VII;

(d) the effectiveness of the enforcement mechanisms, penalty provisions and the accreditation regime;

(e) the performance of the Regulator and the Implementation Authority in discharging their respective functions;

(f) any unintended consequences of this Act; and

(g) whether any amendments to this Act are required.

(3) In conducting the review, the Minister shall consult with—

(a) the Regulator;

(b) relevant government agencies;

(c) civil society organisations;

(d) the private sector; and

(e) credential holders.

(4) The Minister shall, within 6 months after the completion of the review, table a report on the findings and recommendations of the review before the National Parliament.

SCHEDULE 1 — CONSEQUENTIAL AMENDMENTS

1. *National Information and Communication Technology Act* 2009

Amend the *National Information and Communication Technology Act* 2009 by inserting provisions—

(a) designating NICTA as the Regulator for the purposes of the Verifiable Credential and Trust Services Act 2026;

(b) conferring functions, powers and duties necessary to administer the National Digital Identity and Trust Services Framework;

(c) enabling standards-setting, accreditation, supervision, cybersecurity and incident reporting for digital identity and verifiable credentials; and

(d) making such further amendments as are necessary to give full effect to this Act.

2. *Digital Government Act* 2022

Amend the *Digital Government Act* 2022 by inserting provisions—

(a) formalising the role of the Department as policy authority for digital identity and the National Digital Identity and Trust Services Framework;

(b) enabling the designation framework for the Implementation Authority;

(c) providing for coordinated multi-stakeholder governance arrangements;

(d) enabling SevisPass-based single sign-on for appropriate government digital platforms; and

(e) making such further amendments as are necessary to give effect to this Act.

3. *Civil and Identity Registration Act* 2024

Amend the *Civil and Identity Registration Act* 2024 by inserting provisions—

(a) enabling lawful data-sharing arrangements between the civil registry and the National Digital Identity and Trust Services Framework through SevisDEx, subject to consent and data protection safeguards;

(b) clarifying that SevisPass complements and does not duplicate or replace the civil registry; and

(c) making such further amendments as are necessary to give effect to this Act.

4. *Other Acts*

Review and amend, as necessary, the following Acts and related legislation to enable issuance, recognition, verification or presentation of prescribed credentials under this Act—

(a) the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015;

(b) the *Road Traffic Act* 2014;

(c) the *Immigration and Citizenship Service Authority Act* 2010 and related migration legislation;

(d) the *Income Tax (2018 Budget) (Amendment) Act* 2017 and related Internal Revenue Commission enabling laws;

(e) the *Education Act* 1983;

(f) the *Higher Education (General Provisions) Act* 2014;

(g) the *Police Act* 1998;

(h) the *Employment of Non-Citizens Act* 2007;

(i) the *Superannuation (General Provisions) Act* 2000; and

(j) professional registration laws and any other related laws..

SCHEDULE 2 — NATIONAL DIGITAL IDENTITY AND TRUST SERVICES FRAMEWORK FOUNDATIONAL PRINCIPLES

1. Foundational principles

The National Digital Identity and Trust Services Framework established under this Act shall be administered consistently with the following principles:

(a) legality and constitutional compliance;

(b) user-centric design and enforceable holder rights;

(c) privacy by design and data minimisation;

(d) purpose limitation and lawful consent;

(e) security, resilience and cybersecurity by design;

(f) interoperability and open standards, where appropriate;

(g) selective disclosure and proportionality of data sharing;

(h) inclusion, accessibility and accommodation for vulnerable persons;

(i) State sovereignty and control over core trust infrastructure;

(j) accountability, transparency and auditability;

(k) continuity of service and portability; and

(l) phased, practical and sector-sensitive implementation.

2. Effect of Schedule

This Schedule guides the interpretation and administration of this Act and any regulation, standard, code, approval, accreditation condition or decision made under it.