INDEPENDENT STATE OF PAPUA NEW GUINEA

Proposed Draft (Fourth Draft) For External Consultation

No. __ of 2026.
A BILL
For
AN ACT entitled

CYBERSECURITY ACT 2026

Certified on: __ / __ /2026.

No. __ of 2026.

A BILL

For

AN ACT entitled

CYBERSECURITY ACT 2026

ARRANGEMENT OF SECTIONS

INDEPENDENT STATE OF PAPUA NEW GUINEA

No. of 2026.

CYBERSECURITY ACT 2026

Being an Act -

a) to provide for a comprehensive national cybersecurity framework for Papua New Guinea;
b) to vest NICTA with the functions and powers of the National Cybersecurity Authority until a separate Authority is established by NEC decision and notice in the National Gazette;
c) to provide for the establishment of a separate National Cybersecurity Authority when so directed by the National Executive Council;
d) to designate and protect critical information infrastructure;
e) to prevent and penalise cybercrime; to protect financial systems and children online;
f) to vest all cybercrime investigation functions in the Cybercrime Investigation Unit of the Royal Papua New Guinea Constabulary;
g) to regulate investigation powers and the admissibility of digital evidence;
h) to impose obligations on digital platform and ICT service providers;
i) to provide for international cooperation in cybersecurity matters; and

for related purposes.

MADE by the National Parliament to come into operation in accordance with a Notice in the National Gazette by the Head of the State, acting with, and in accordance with, the advice of the Minister.

Certified on: / / 2026
Speaker of the National Parliament

PART I - PRELIMINARY

1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS.

(1) This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III.3.C (qualified rights) of the Constitution, namely —

(a) the right to freedom from arbitrary search and entry conferred by Section 44; and
(b) the right to freedom of expression conferred by Section 46; and
(c) the right to peaceful assembly and association conferred by Section 47; and
(d) the right to privacy conferred by Section 49; and
(e) the right to freedom of information conferred by Section 51,

is a law that is made for the purpose of giving effect to the public interest in public order and public welfare.

(2) For the purposes of Section 41 of the Organic Law on Provincial Governments and Local-level Governments, it is declared that this Act relates to a matter of national interest.

(3) For the purposes of Section 53(1) of the Constitution, the purposes of this Act, including the freezing of electronic assets under Section 45 and the giving of emergency directions under Part XI, are declared to be public purposes.

2. COMMENCEMENT.

(1) This Act comes into operation on the date of certification.

(2) Parts II, Sections 13 to 24 come into operation on a day to be fixed by the Head of State, acting on advice, by notice published in the National Gazette.

(3) For clarity, Part II, which deems NICTA to be the National Cybersecurity Authority, comes into operation on the date of certification of this Act, so that NICTA may immediately begin performing the functions and exercising the powers of the Authority.

3. INTERPRETATION.

(1) In this Act, unless the contrary intention appears —

(a) "***AI system***" means an automated system that uses machine learning, neural networks, or similar technologies to generate output including predictions, recommendations, decisions, or synthetic content;
(b) "***Authority"*** means NICTA, in its capacity as the deemed National Cybersecurity Authority under Section 7, until a separate National Cybersecurity Authority is established under Section 8; or the separate National Cybersecurity Authority established under Section 8, from the date of its establishment;
(c) "***authorised investigator***" means a person designated under Section 73;
(d) "***Board***" means, in the interim period NICTA Board or when a separate National Cybersecurity Authority has been established under Section 8, the Board of Directors of that Authority established under Section 13;
(e) "***Budapest Convention***" means the Convention on Cybercrime (ETS No. 185) of the Council of Europe opened for signature on 23 November 2001;
(f) "***CERT***" means the Papua New Guinea Computer Emergency Response Team established by Section 26;
(g) "***Chief Executive Officer***" means the Chief Executive Officer of NICTA in the interim period or the Chief Executive Officer appointed under Section 17;
(h) "**child**" means a person who has not attained the age of 18 years;
(i) "***CII operator***" means a person or entity that owns, manages, or controls a designated critical information infrastructure facility, system, or service;
(j) "***Commissioner***" means the Child Online Safety Commissioner designated under Section 54;
(k) "***computer system***" means any electronic device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data, and includes —

(i) a personal computer, server, or mobile device;
(ii) a network of devices;
(iii) cloud computing infrastructure;
(iv) an Internet of Things device;
(v) an operational technology or SCADA system; and
(vi) any data storage device;

(l) "critical information infrastructure" or "CII" means any computer system, network, facility, or service designated under Section 31;

(m) "***cybercrime***" means an offence committed using an electronic device, system, or network;

(n) "***cybersecurity***" means the collection of tools, policies, safeguards, guidelines, risk management approaches, training, and technologies used to protect computer systems, networks, and data from attack, damage, or unauthorised access;

(o) "***cybersecurity incident***" or "***incident***" means —
(i) any breach, compromise, or disruption affecting the confidentiality, integrity, or availability of a computer system or the data it holds; or
(ii) any attempted breach that poses a significant risk to a computer system;

(p) "***data*"** means any representation of information, knowledge, facts, concepts, or instructions, whether in a form suitable for use in a computer system or not;

(q) "***personal data breach***" has the same meaning as "data breach" in Section 3 of the Data Governance and Data Protection Act 2026, being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; and all references in this Act to "data breach" shall be read as references to "personal data breach";

(r) "***deepfake***" means a synthetic audio, video, image, or text generated by an AI system that depicts or purports to depict a real person doing or saying something the person did not do or say;

(s) "***Department***" means the Department of Information and Communications Technology;

(t) "***digital evidence***" has the meaning given by Section 77;

(u) "electronic communication" means a communication transmitted by means of a computer system or a telecommunications network;

(v) "***financial institution***" means a bank, insurance company, savings and loan society, micro-finance institution, payment service provider, or other entity licensed by the Bank of Papua New Guinea to conduct financial services;

(w) "***malware***" means any software designed to damage, disrupt, gain unauthorised access to, or extract data from a computer system, and includes ransomware, spyware, trojans, viruses, worms, keyloggers, and rootkits;

(x) "***Minister***" means the Minister responsible for information and communications technology;

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

(ya) "***NICTA Act***" means the National Information and Communications Technology Act 2009;

(z) "***operator***" means a person or entity that owns, manages, or controls a computer system or network;

(za) "personal data" has the same meaning as in Section 3 of the Data Governance and Data Protection Act 2026;

(zb) "***platform"*** means a social media platform as defined by Section 48;

(zc) "***prescribed***" means prescribed by or under a regulation made under this Act;

(zd) "***ransomware***" means malware that encrypts or restricts access to a computer system or data and demands payment for restoration of access;

(ze) "***sensitive personal data***" has the same meaning as in Section 51 of the Data Governance and Data Protection Act 2026; and all references in this Act to "sensitive information" shall be read as references to "sensitive personal data";

(zf) "***Unit***" means the Cybercrime Investigation Unit of the Royal Papua New Guinea Constabulary established by Section 63.

3A. DATA CONTROLLERS AND DATA PROCESSORS.

(1) This section applies where personal data is collected, used, disclosed, retained or otherwise processed under or for the purposes of this Act.

(2) A person who, alone or jointly with another person, determines the purposes and means of the processing is the data controller for the purposes of the Data Governance and Data Protection Act 2026.

(3) A person who processes the personal data on behalf of the data controller is the data processor for the purposes of that Act.

(4) The data controller and the data processor must comply with the Data Governance and Data Protection Act 2026 in relation to the processing.

4. APPLICATION.

(1) This Act applies throughout Papua New Guinea and, to the extent provided by this section, outside Papua New Guinea.

(2) This Act applies to —

(a) a person in Papua New Guinea; and

(b) a citizen or permanent resident of Papua New Guinea who is outside Papua New Guinea, to the extent permitted by international law; and

(c) a computer system located in Papua New Guinea, and a computer system owned or operated by the State or a public body, wherever located; and

(d) a person outside Papua New Guinea whose act or omission is directed at, or affects, a computer system, data or a person in Papua New Guinea.

(3) This Act applies to an act or omission that occurs after the commencement of the provision that creates the relevant duty, obligation or offence.

(4) This Act does not limit or restrict a right or freedom conferred by the Constitution except to the extent permitted by Section 38 of the Constitution and declared in Section 1.

5. OBJECTS OF THE ACT.

(1) The objects of this Act are to —

(a) establish a comprehensive national framework for cybersecurity that is consistent with the Constitution of Papua New Guinea and the National Cybersecurity Policy 2021;

(b) vest NICTA with the functions and powers of the National Cybersecurity Authority until a separate Authority is established by the National Executive Council by notice in the National Gazette;

(c) designate and protect critical information infrastructure vital to national security, economy, and public safety;

(d) protect Papua New Guinea's financial systems from cybercrime;

(e) protect children from online harm, including by restricting access to social media platforms;

(f) formally establish a Cybercrime Investigation Unit with provincial presence to investigate serious cybercrime;

(g) provide clear investigation powers and digital evidence rules to support effective prosecution;

(h) create comprehensive, graduated cybercrime offences reflecting current and emerging threats;

(i) impose obligations on digital platforms and ICT service providers;

(j) provide for international cooperation in combating cybercrime; and

(k) build national cybersecurity capacity and public awareness.

6. ACT BINDS THE STATE.

This Act binds the State.

PART II - NICTA AS NATIONAL CYBERSECURITY

7. NICTA DEEMED TO BE THE AUTHORITY.

(1) NICTA is deemed to be the National Cybersecurity Authority for the purposes of this Act.
(2) Until a separate National Cybersecurity Authority is established under Section 8 —
  (a) NICTA performs all functions of the Authority under this Act;
  (b) NICTA exercises all powers of the Authority under this Act;
  (c) all references in this Act to 'the Authority' are to be read as references to NICTA; and
  (d) the NICTA Board of Directors performs the functions of the Board under this Act, and the Chief Executive Officer of NICTA performs the functions of the Chief Executive Officer of the Authority.
(3) NICTA, in performing functions and exercising powers under this Act, acts under the governance, direction, and accountability framework of the NICTA Act, as supplemented by this Act.
(4) The functions and powers conferred on NICTA under this Act are in addition to, and do not limit, the functions and powers of NICTA under the NICTA Act.
(5) NICTA must —
  (a) establish a dedicated Cybersecurity Division within its organisational structure for the performance of its functions under this Act; and
  (b) designate a senior officer of NICTA as the Cybersecurity Division Director responsible for the day-to-day administration of NICTA's functions under this Act.
(6) In exercising functions under this Act that involve personal data, NICTA and any successor Authority remain subject to the Data Governance and Data Protection Act 2026, including obligations relating to lawfulness, data minimisation, integrity, confidentiality, storage limitation and accountability.

8. ESTABLISHMENT OF SEPARATE NATIONAL CYBERSECURITY AUTHORITY.

(1) The National Executive Council may, at any time, by decision, direct that a separate National Cybersecurity Authority be established for the purposes of this Act.
(2) Upon a decision of the National Executive Council under Subsection (1), the Minister must cause a notice to be published in the National Gazette —
  (a) establishing the National Cybersecurity Authority as a body corporate with perpetual succession, a common seal, and capacity to sue and be sued in its corporate name;
  (b) stating the date from which the separate Authority is established; and
  (c) stating the date from which NICTA's deemed status as the Authority ceases.
(3) From the date specified in the Gazette notice under Subsection (2) —
  (a) NICTA's deemed status as the Authority under Section 7 ceases;
  (b) the separate National Cybersecurity Authority assumes all functions and powers of the Authority under this Act;
  (c) the separate Authority becomes the Authority for all purposes of this Act; and
  (d) the governance provisions in Sections 13 to 24 apply to the separate Authority.

9. TRANSFER OF FUNCTIONS AND ASSETS TO SEPARATE AUTHORITY.

(1) Upon the establishment of a separate National Cybersecurity Authority under Section 8 -
  (a) all assets held by NICTA exclusively for the purposes of this Act vest in the separate Authority;

(b) all liabilities of NICTA incurred exclusively in the performance of its functions under this Act become liabilities of the separate Authority;
(c) all staff of NICTA engaged exclusively in performing functions under this Act may, with their consent, be transferred to the employment of the separate Authority on terms no less favourable than those applicable immediately before the transfer;
(d) all agreements, contracts, and arrangements entered into by NICTA in the performance of its functions under this Act have effect as if entered into by the separate Authority; and
(e) all proceedings pending by or against NICTA in relation to its functions under this Act may be continued by or against the separate Authority.

(2) NICTA and the separate Authority must cooperate to ensure an orderly and efficient transition of functions.

10. FUNCTIONS OF THE AUTHORITY.

(1) The functions of the Authority are to —
(a) coordinate the implementation of national cybersecurity policy and strategy;
(b) develop, issue, and enforce national cybersecurity standards and guidelines;
(c) designate and oversee the protection of critical information infrastructure;
(d) operate the Cybersecurity Response Centre and coordinate national incident response;
(e) regulate and licence cybersecurity service providers;
(f) certify and maintain a register of cybersecurity professionals;
(g) promote cybersecurity awareness, education, and capacity building;
(h) advise the Minister on cybersecurity matters, legislation, and policy;
(i) facilitate national and international cybersecurity cooperation;
(j) monitor and assess cybersecurity threats and publish threat advisories;
(k) administer the child online safety framework under Part VI; and
(l) perform any other function conferred on the Authority by or under this Act.

(2) For clarity, the Authority does not perform cybercrime investigation functions. All cybercrime investigation functions are performed exclusively by the Unit under Part VII.

11. POWERS OF THE AUTHORITY.

(1) The Authority has power to do all things necessary or convenient to be done for or in connection with the performance of its functions.

(2) Without limiting Subsection (1), the Authority may -
(a) enter into contracts and arrangements;
(b) accept grants, donations, and contributions;
(c) issue compliance orders to any person or entity subject to this Act;
(d) conduct inspections and audits of computer systems subject to this Act;
(e) require the production of documents or information relevant to its functions;
(f) refer matters for investigation to the Unit; and
(g) do anything else authorised by this Act or the regulations.

12. MINISTERIAL DIRECTIONS.

(1) The Minister may, by written notice, give directions to the Authority with respect to the performance of its functions and the exercise of its powers under this Act.

(2) The Authority must comply with a direction given under Subsection (1).

(3) A direction under Subsection (1) must not relate to a specific enforcement action or compliance matter against a particular person.

(4) Where NICTA is acting as the Authority under Section 7, a direction under this section is given to NICTA and is in addition to any Ministerial direction that may be given to NICTA under the NICTA Act.

13. BOARD OF SEPARATE NATIONAL CYBERSECURITY AUTHORITY.

(1) Upon its establishment, the separate National Cybersecurity Authority has a Board of Directors.

(2) The Board consists of —

(a) a Chairperson, who must have expertise in cybersecurity, law, or public administration; and

(b) eight other members, of whom —

(i) one must be a representative of NICTA nominated by the NICTA Board;

(ii) one must be a representative of the Bank of Papua New Guinea nominated by the Governor;

(iii) one must be a representative of the Royal Papua New Guinea Constabulary nominated by the Commissioner of Police;

(iv) one must be a representative of the Department nominated by the Secretary;

(v) one must be a representative of the private ICT sector nominated by the relevant industry body;

(vi) one must be a person with expertise in child protection nominated by the relevant civil society organisation;

(vii) one must be a person with expertise in cybersecurity law or constitutional law; and

(viii) one must be a woman with relevant expertise,

appointed by the Head of State, acting on advice of the National Executive Council, on the recommendation of the Minister.

14. QUALIFICATIONS OF BOARD MEMBERS.

(1) A person is not eligible for appointment as a member of the Board of the separate Authority unless the person has relevant qualifications or experience in cybersecurity, information technology, law, finance, or public administration.

(2) A person is not eligible if the person —

(a) is an undischarged bankrupt;

(b) has been convicted of an offence punishable by imprisonment; or

(c) has a disqualifying conflict of interest in relation to the functions of the Authority.

15. TENURE OF BOARD MEMBERS.

(1) A member of the Board of the separate Authority holds office for a term of 3 years and is eligible for reappointment for one further term only.

(2) A person must not hold office as a member of the Board for more than 6 years in total.

(3) A member may resign from office by written notice delivered to the Minister.

16. VACATION OF OFFICE.

(1) A member of the Board of the separate Authority vacates office if the member —

(a) dies;

(b) resigns in accordance with Section 15(3);

(c) becomes an undischarged bankrupt;

(d) is convicted of an offence punishable by imprisonment; or

(e) is removed from office by the Head of State, acting on advice of the National Executive Council, on the recommendation of the Minister, on the ground that the member is incapable of satisfactorily performing the duties of office.

17. MEETINGS OF THE BOARD.

(1) The Board of the separate Authority must hold at least 4 meetings in each calendar year.

(2) Meetings are to be held at times and places determined by the Chairperson.

(3) The Chairperson must convene a special meeting if requested in writing by at least 4 members.
(4) 5 members of the Board constitute a quorum at a meeting.
(5) A question before the Board is decided by a majority of members present and voting.
(6) The Chairperson has a deliberative vote and, in the event of an equality of votes, also has a casting vote.
(7) The Board must cause accurate minutes to be kept of all meetings.

18. DISCLOSURE OF INTEREST.

(1) A member of the Board who has a material personal interest in a matter being considered by the Board must —
    (a) disclose the nature of the interest to the Board before the matter is considered; and
    (b) not take part in the consideration or decision of the matter.
(2) A disclosure under Subsection (1) must be recorded in the minutes of the relevant meeting.

19. CHIEF EXECUTIVE OFFICER OF SEPARATE AUTHORITY.

(1) The separate National Cybersecurity Authority shall have a Chief Executive Officer.
(2) The Chief Executive Officer is appointed by the Minister on the recommendation of the Board.
(3) A person is not eligible for appointment unless the person has —
    (a) relevant qualifications in cybersecurity, information technology, or law; and
    (b) at least 7 years relevant professional experience.
(4) The Chief Executive Officer holds office for a term of 4 years and is eligible for reappointment for one further term only.

20. FUNCTIONS OF CHIEF EXECUTIVE OFFICER.

(1) The Chief Executive Officer is responsible for the day-to-day management and administration of the separate Authority.
(2) The Chief Executive Officer must perform the functions conferred by or under this Act and any functions delegated by the Board.
(3) The Chief Executive Officer is accountable to the Board in the performance of those functions.

21. STAFF OF SEPARATE AUTHORITY.

(1) The separate Authority may employ staff necessary for the performance of its functions.
(2) Staff are employed on terms and conditions determined by the Board in consultation with the relevant public sector employment authority.
(3) The Chief Executive Officer may, by written instrument, delegate any of the Authority's administrative functions to a member of staff.

22. FUNDS AND FINANCIAL PROVISIONS.

(1) While NICTA is performing the functions of the Authority under Section 7, the costs and expenses incurred by NICTA in the performance of those functions are to be met from funds appropriated by the Parliament for the purposes of this Act and allocated to NICTA for that purpose.
(2) NICTA must maintain separate accounts for its activities under this Act, distinguishable from its other accounts under the NICTA Act.
(3) Upon the establishment of the separate Authority under Section 8, the funds of the separate Authority consist of —
    (a) moneys appropriated by the Parliament for the purposes of the separate Authority;
    (b) fees and charges collected by the separate Authority under this Act;
    (c) grants and donations received by the separate Authority with the approval of the Minister; and
    (d) any other moneys lawfully received by or for the separate Authority.
(4) The funds of the separate Authority must be applied only for the purposes of this Act.

23. ANNUAL BUDGET.

(1) While NICTA performs the functions of the Authority under Section 7, NICTA must, before the start of each financial year, include in its annual budget a separate allocation for activities under this Act and submit it to the Minister for approval.
(2) Upon the establishment of the separate Authority under Section 8, the Board of the separate Authority must, before the start of each financial year, prepare and submit to the Minister a proposed budget for that year.
(3) The Minister must approve the budget, with or without amendment, within 60 days of receipt.

24. AUDIT AND ANNUAL REPORT.

(1) The accounts relating to activities under this Act are subject to inspection and audit by the Auditor-General under the Audit Act (Chapter 444).
(2) The Authority must, within 3 months after the end of each financial year, prepare and submit to the Minister an annual report on its operations under this Act during that year.
(3) The annual report must include —
    (a) a report on the performance of the Authority's functions under this Act;
    (b) statistics on cybersecurity incidents reported and responses coordinated;
    (c) a summary of licensing and accreditation activities;
    (d) audited accounts for activities under this Act; and
    (e) such other matters as the Minister directs.
(4) The Minister must table a copy of the annual report in the Parliament within 30 days of receiving it.

PART III - NATIONAL CYBERSECURITY FRAMEWORK AND STRATEGY

25. NATIONAL CYBERSECURITY POLICY.

(1) The Authority must implement this Act in a manner consistent with the National Cybersecurity Policy as approved by the National Executive Council from time to time.
(2) Where there is an inconsistency between the National Cybersecurity Policy and the provisions of this Act, this Act prevails.

26. NATIONAL CYBERSECURITY STRATEGY.

(1) The Minister must, on the advice of the Authority, approve a National Cybersecurity Strategy within 12 months of the commencement of this Part.
(2) The National Cybersecurity Strategy must —
    (a) set out the national priorities for cybersecurity for a 3-year period;
    (b) identify key risks and threats to Papua New Guinea's cyberspace;
    (c) establish goals and measurable targets for each priority area;
    (d) assign responsibilities to government agencies and other stakeholders; and
    (e) provide for resourcing and implementation.
(3) The Minister must table the National Cybersecurity Strategy in the Parliament within 30 days of its approval.
(4) The Authority must review and update the National Cybersecurity Strategy every 3 years.

27. NATIONAL CYBERSECURITY COORDINATION COMMITTEE.

(1) The National Cybersecurity Coordination Committee is established.
(2) The Committee consists of —
    (a) the Chief Executive Officer of NICTA (or, when a separate Authority is established, the Chief Executive Officer of that Authority), who is the Chairperson;
    (b) a representative of the Department of Defence;
    (c) a representative of the National Intelligence Organisation;
    (d) the Commander of the Cybercrime Investigation Unit;
    (e) a representative of the Department of Justice and Attorney General;
    (f) a representative of the Bank of Papua New Guinea;
    (g) a representative of the Office of Censorship; and
    (h) a representative of the Office of Security Coordination and Assessment.
(3) The Committee must meet at least quarterly.
(4) The functions of the Committee are to —
    (a) coordinate cybersecurity activities across government agencies;
    (b) share threat intelligence and incident information to the extent necessary for cybersecurity purposes and, where such information contains personal data, only in a form that is proportionate and, where feasible, redacted, pseudonymised or anonymised, and otherwise in accordance with the Data Governance and Data Protection Act 2026; and
    (c) advise the Minister and the National Executive Council on matters requiring whole-of-government response.

28. PAPUA NEW GUINEA COMPUTER EMERGENCY RESPONSE TEAM.

(1) The Papua New Guinea Computer Emergency Response Team (PNGCERT) is established within NICTA.
(2) Upon the establishment of a separate Authority under Section 8, the PNGCERT transfers to and continues to operate within the separate Authority.
(3) The CERT has the following functions —
    (a) receive, analyse, and coordinate responses to cybersecurity incidents;
    (b) issue alerts and advisories on cybersecurity threats;

(c) provide technical assistance to entities affected by cybersecurity incidents;
(d) liaise with international CERTs and cybersecurity bodies; and
(e) promote cybersecurity situational awareness nationally and regionally.

(4) The CERT shall operate on a 24-hours-a-day, 7-days-a-week basis.

31. CYBERSECURITY OPERATIONS CENTRE.

(1) The Authority must establish and operate a Cybersecurity Operations Centre.

(2) The Cybersecurity Operations Centre has the following functions —
(a) monitor network traffic and security events within government information systems;
(b) detect and analyse cybersecurity threats and incidents in real time;
(c) provide threat intelligence to the CERT and relevant agencies; and
(d) support post-incident analysis and forensic review.

(3) The existing National Cybersecurity Centre established within NICTA with Australian Government support in 2018 is taken to be the Cybersecurity Operations Centre for the purposes of this section until the Authority establishes a replacement Centre.

32. CYBERSECURITY STANDARDS.

(1) The Authority may, by notice published in the National Gazette, issue minimum cybersecurity standards applicable to —
(a) all government agencies and public bodies;
(b) designated CII operators;
(c) licensed cybersecurity service providers; and
(d) any other class of person specified in the notice.

(2) Cybersecurity standards issued under this section must be consistent with internationally recognised standards including the NIST Cybersecurity Framework, ISO/IEC 27001, or their successors.

(3) A person subject to a cybersecurity standard issued under Subsection (1) must comply with that standard.

PART IV - CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

31. DESIGNATION OF CRITICAL INFORMATION INFRASTRUCTURE.

(1) The Minister may, on the advice of the Authority, by notice published in the National Gazette, designate any computer system, network, facility, or service as critical information infrastructure for the purposes of this Act.

(2) In designating critical information infrastructure, the Minister must consider —

- (a) the number of persons who would be adversely affected if the system were disrupted;
- (b) cross-sector interdependencies;
- (c) risks to national security, public health, or public safety; and
- (d) impact on essential public services.

(3) The following categories of infrastructure are taken to be designated critical information infrastructure unless otherwise specified by the Minister —

- (a) banking and financial systems;
- (b) telecommunications networks;
- (c) energy and power generation and distribution systems;
- (d) transportation systems including air traffic control, maritime, and road management;
- (e) water and sanitation systems;
- (f) public health and hospital systems;
- (g) government information and communications systems;
- (h) extractive industry operational technology systems; and
- (i) educational institutions,

as further described in Schedule 1.

(4) The Minister may, by notice in the National Gazette, vary or remove a designation made under this section.

32. OBLIGATIONS OF CII OPERATORS.

A CII operator must —

- (a) implement the minimum cybersecurity controls prescribed by the Authority under Section 28;
- (b) appoint a Cybersecurity Officer in accordance with Section 33;
- (c) conduct annual risk assessments in accordance with Section 34;
- (d) report cybersecurity incidents to the Authority in accordance with Section 35;
- (e) submit to compliance audits conducted by the Authority under Section 36;
- (f) comply with ICT supply chain security requirements under Section 37; and
- (g) cooperate with the Authority in the exercise of its functions under this Act.

33. CYBERSECURITY OFFICER.

(1) A CII operator must appoint a person as Cybersecurity Officer for each CII facility or system.

(2) A Cybersecurity Officer must have relevant qualifications and experience in cybersecurity, as prescribed.

(3) The Cybersecurity Officer is responsible for —

- (a) overseeing the cybersecurity of the CII facility or system;
- (b) implementing and maintaining cybersecurity controls;
- (c) coordinating incident response and reporting; and
- (d) providing cybersecurity advice to the management of the CII operator.

(4) A CII operator must notify the Authority in the prescribed manner of the appointment of a Cybersecurity Officer within 30 days of appointment.

34. ANNUAL RISK ASSESSMENT.

(1) A CII operator must conduct a comprehensive cybersecurity risk assessment of each designated CII facility or system at least once in each calendar year.

(2) The risk assessment must be conducted in accordance with the standards prescribed by the Authority.
(3) A CII operator must submit a summary of the risk assessment to the Authority within 30 days of its completion.

35. CII INCIDENT REPORTING.

(1) A CII operator that becomes aware of a cybersecurity incident affecting a designated CII facility or system must notify the Authority within 24 hours of becoming aware.
(2) A notification under Subsection (1) must include —
  (a) a description of the incident;
  (b) the date and time the incident was discovered;
  (c) the CII facility or system affected;
  (d) the likely impact of the incident; and
  (e) the measures taken or proposed to mitigate the incident.
(3) A CII operator must provide a full incident report to the Authority within 7 days of the incident.
(4) Where a cybersecurity incident involves personal data, compliance with reporting obligations under this section does not remove or limit the obligation to notify a personal data breach under the Data Governance and Data Protection Act 2026. A report under this section may satisfy that obligation only if it contains the information required under that Act.
(5) Where a reported cybersecurity incident is likely to result in a high risk to the rights or freedoms of affected individuals, the responsible entity must notify affected data subjects without undue delay in accordance with Section 64 of the Data Governance and Data Protection Act 2026, unless an exemption under that Act or a lawful investigative restriction applies.

36. COMPLIANCE AUDIT.

(1) The Authority may, at any time, audit the cybersecurity measures and practices of a CII operator.
(2) An authorised officer conducting an audit may —
  (a) enter and inspect premises of the CII operator;
  (b) inspect, copy, and take extracts of records and systems; and
  (c) require the CII operator or any employee to answer questions and produce documents.
(3) A CII operator must cooperate with an audit conducted under this section.

37. ICT SUPPLY CHAIN SECURITY.

(1) A CII operator must not procure or deploy ICT products or services in a CII facility or system unless satisfied that the product or service meets the prescribed cybersecurity requirements.
(2) The Minister may, on the advice of the Authority, by notice in the National Gazette, prohibit the use of specified ICT products or services in CII facilities or systems on national security grounds.

38. GOVERNMENT ASSISTANCE FOR CII.

(1) Where a cybersecurity incident affecting CII poses or may pose a serious risk to national security or essential services, the Authority may, with the approval of the Minister, provide direct technical assistance to the CII operator.
(2) A CII operator must not unreasonably refuse government assistance provided under Subsection (1).

39. OFFENCE — FAILURE TO COMPLY WITH CII OBLIGATIONS.

(1) A CII operator that, without reasonable excuse, fails to comply with a requirement imposed by this Part commits an offence.

Penalty: A fine not exceeding K200,000 or imprisonment for a term not exceeding 5 years, or both.

(2) In the case of a body corporate, the fine is not exceeding K1,000,000.

PART V - PROTECTION OF FINANCIAL SYSTEMS

40. DESIGNATION OF FINANCIAL SYSTEMS AS CRITICAL INFRASTRUCTURE.

(1) All computer systems and networks operated by financial institutions are taken to be designated critical information infrastructure for the purposes of this Act.
(2) In addition to the obligations in Part IV, financial institutions are subject to the obligations in this Part.

41. OBLIGATIONS OF FINANCIAL INSTITUTIONS.

A financial institution must —
- (a) implement the minimum cybersecurity controls prescribed for financial institutions by the Authority, in consultation with the Bank of Papua New Guinea;
- (b) report a cybersecurity incident affecting its systems to both the Authority and the Bank of Papua New Guinea within 24 hours of detection;
- (c) maintain an incident response plan specifically addressing financial cybercrime;
- (d) conduct regular penetration testing of its systems; and
- (e) train staff in cybersecurity awareness and fraud prevention.

(5) Where a cybersecurity incident under this section involves personal data, compliance with reporting obligations under this section does not remove or limit the obligation to notify a personal data breach under the Data Governance and Data Protection Act 2026. A report under this section may satisfy that obligation only if it contains the information required under that Act.
(6) Where a reported incident is likely to result in a high risk to the rights or freedoms of affected individuals, the responsible entity must notify affected data subjects without undue delay in accordance with Section 64 of the Data Governance and Data Protection Act 2026, unless an exemption under that Act or a lawful investigative restriction applies.

42. FINANCIAL CYBERCRIME OFFENCES.

(1) A person who, by means of a computer system, gains unauthorised access to the computer systems of a financial institution with intent to —
- (a) obtain money, property, or financial advantage by deception;
- (b) manipulate financial records or transactions; or
- (c) disrupt the provision of financial services,
- (0) commits an offence.

Penalty: A fine not exceeding K1,000,000 or imprisonment for a term not exceeding 20 years, or both.

(2) In the case of a body corporate, A fine is not exceeding K5,000,000.

43. IDENTITY THEFT AND PHISHING OFFENCES.

(1) A person who dishonestly —
- (a) obtains another person's identification information or financial credentials by means of a computer system; or
- (b) sends or causes to be sent an electronic communication falsely purporting to be from a financial institution, government body, or other trusted entity, with intent to induce the recipient to disclose personal or financial data,

commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

(2) It is not a defence to a charge under Subsection (1) that the offender did not directly use the information obtained.

44. ELECTRONIC FRAUD.

(1) A person who, with intent to defraud, uses a computer system to —
(a) input, alter, delete, or suppress data;
(b) interfere with the functioning of a computer system; or
(c) cause a financial loss to another person or financial gain to the person or another,
commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

45. FREEZING OF ELECTRONIC ASSETS.

(1) Where the Authority or the Unit has reasonable grounds to believe that funds held in an electronic account or digital wallet are proceeds of a cybercrime offence, the Authority may apply to the National Court for an order freezing those assets.
(2) An application under Subsection (1) may be made ex parte where there is a risk that assets will be dissipated.
(3) An order under this section may be made for an initial period not exceeding 30 days and may be renewed by the Court.

46. COOPERATION WITH BANK OF PAPUA NEW GUINEA.

(1) The Authority must enter into a written cooperation agreement with the Bank of Papua New Guinea for the purposes of this Part.
(2) The cooperation agreement must provide for —
(a) sharing of cybersecurity threat intelligence relating to the financial sector;
(b) coordinated incident response for financial system cyberattacks; and
(c) joint review of cybersecurity standards applicable to financial institutions.

47. COOPERATION WITH FINANCIAL ANALYSIS AND SUPERVISION UNIT.

(1) The Authority must cooperate with the Financial Analysis and Supervision Unit established under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 in relation to —
(a) cybercrime offences involving money laundering or terrorist financing; and
(b) the freezing and recovery of assets obtained through financial cybercrime.

PART VI - CHILD ONLINE SAFETY AND SOCIAL MEDIA REGULATION

48. INTERPRETATION — PART VI.

In this Part, unless the contrary intention appears —

(a) "***age verification"*** means a method used to determine or estimate the age or age range of a user of an online service;

(b) "***high-risk platform***" means a social media platform that enables contact with unknown persons, exposes users to harmful content, facilitates exploitation of children as consumers, or poses risks to children's personal data, mental health, or psychological wellbeing;

(c) "***ordinary resident***" means a child ordinarily resident in Papua New Guinea for the purposes of determining the application of this Part;

(d) "***social media platform***" means an online service that —

(i) enables two or more users to create accounts;

(ii) allows users to interact with, share content with, or follow other users; and

(iii) allows users to post, upload, view, or share material,

and includes the platforms set out in Schedule 1 Part B;

(e) "social media account" means an account created by a user on a social media platform.

49. MINIMUM AGE FOR SOCIAL MEDIA ACCOUNTS.

(1) A social media platform must not allow a child who is an ordinary resident of Papua New Guinea to create or maintain a social media account on the platform.

(2) Subsection (1) applies to children under the age of 16 years.

(3) The onus of compliance with this section is on the social media platform, not on the child or the child's parents or guardians.

50. OBLIGATIONS OF SOCIAL MEDIA PLATFORMS.

(1) A social media platform operating in or accessible from Papua New Guinea must -

(a) implement reasonable steps to prevent children under 16 years from creating or maintaining accounts on the platform;

(b) establish age verification systems that are reasonable, effective, and privacy-preserving;

(c) take down the account of any user the platform knows or ought reasonably to know is a child;

(d) configure privacy settings for users under 18 years at the highest protective level by default;

(e) not use profiling, behavioural advertising, or engagement-maximising design features targeting children;

(f) not use covert methods to encourage children to disclose personal information; and

(g) provide a clear, accessible mechanism for reporting harmful content involving children.

51. AGE VERIFICATION REQUIREMENTS.

A social media platform must implement age verification measures that —

(a) are reasonably effective at preventing children under 16 from holding accounts;

(b) are proportionate to the privacy interests of users;

(c) do not require a user to provide government-issued identification unless the user elects to do so; and

(d) offer at least one alternative age verification method that does not require government identification.

52. PRIVACY OF AGE VERIFICATION DATA.

A social media platform or age verification provider that collects personal data for the purpose of age verification must —

(a) use the data only for the purpose of age verification;
(b) not retain the data after verification is complete; and
(c) destroy the data in accordance with the prescribed standards.

(4) Any collection, use, storage, disclosure or destruction of age verification data under this section must also comply with the Data Governance and Data Protection Act 2026, including any special protections applicable to children's personal data, biometric data and sensitive personal data. Such data must not be used for profiling, marketing, behavioural analytics, or any unrelated purpose.

53. EXEMPTIONS.

Section 49 does not apply to —

(a) a messaging application that does not allow public posting of content;
(b) an online platform used primarily for educational or professional development purposes;
(c) a health support or mental health service platform;
(d) an online gaming platform that does not include significant social media features; or
(e) any other service specified by the Commissioner by notice in the National Gazette.

54. CHILD ONLINE SAFETY COMMISSIONER.

(1) The Minister must designate a person as the Child Online Safety Commissioner.
(2) The Commissioner is responsible for —

(a) administering and enforcing this Part;
(b) assessing compliance of social media platforms with this Part;
(c) investigating complaints relating to online harm to children;
(d) issuing removal notices under Section 61;
(e) providing guidance to platforms on compliance;
(f) coordinating with the Unit on grooming and CSEM investigations; and
(g) reporting annually to the Minister on child online safety in Papua New Guinea.

55. ONLINE GROOMING.

(1) A person who, using an electronic communication, communicates with a child under the age of 16 years for the purpose of facilitating the commission of a sexual offence against that child, or against any other child, commits an offence.

Penalty: Imprisonment for a term not exceeding 15 years.

(2) It is not a defence to a charge under Subsection (1) that the child was a fictitious person represented as a real child.

56. CHILD SEXUAL EXPLOITATION MATERIAL.

(1) A person who, by means of a computer system —

(a) produces, makes, generates, or creates child sexual exploitation material;
(b) distributes, transmits, or makes available child sexual exploitation material;
(c) accesses, downloads, or views child sexual exploitation material; or
(d) possesses child sexual exploitation material,

commits an offence.

Penalty: Imprisonment for a term not exceeding life.

(2) In this section, "child sexual exploitation material" means material that depicts or describes, in a way that a reasonable person would find offensive, a child under the age of 18 years engaged in, or appearing to engage in, sexual conduct.

57. CYBERBULLYING OF A CHILD.

A person who, using a computer system, sends a communication to or about a child that causes the child serious emotional or psychological harm, or is likely to do so, commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 3 years, or both.

58. NON-CONSENSUAL SHARING OF INTIMATE IMAGES.

A person who, without the consent of another person, transmits, posts, publishes, or causes to be transmitted an intimate image of that other person using a computer system commits an offence.

Penalty: A fine not exceeding K200,000 or imprisonment for a term not exceeding 5 years, or both.

59. HARMFUL CONTENT TARGETING CHILDREN.

A social media platform that knowingly allows content that sexualises children, promotes eating disorders, self-harm, or suicide to children, or facilitates the exploitation of children, to remain accessible after having received a removal notice under Section 61, commits an offence.

Penalty: A fine not exceeding K5,000,000 for each day the non-compliance continues.

60. REPORTING OBLIGATIONS FOR PLATFORMS — CHILD SAFETY.

A social media platform that discovers child sexual exploitation material on its platform must —

(a) remove the material immediately;
(b) preserve the relevant data; and
(c) report the matter to the Unit within 24 hours.

61. REMOVAL NOTICES.

(1) The Commissioner may issue a written removal notice to a social media platform requiring the platform to remove specified content within 24 hours.
(2) A social media platform that fails to comply with a removal notice without reasonable excuse commits an offence.

Penalty: A fine not exceeding K1,000,000 per day of non-compliance.

62. OFFENCE — NON-COMPLIANCE BY PLATFORM.

(1) A social media platform that, without reasonable excuse, fails to comply with Section 49 or 48 commits an offence.

Penalty: A fine not exceeding K5,000,000 for a first offence, and K10,000,000 for each subsequent offence.

PART VII - CYBERCRIME INVESTIGATION UNIT

63. ESTABLISHMENT OF THE CYBERCRIME INVESTIGATION UNIT.

(1) The Cybercrime Investigation Unit is established within the Royal Papua New Guinea Constabulary.
(2) The Unit shall be commanded by a senior officer of the Royal Papua New Guinea Constabulary holding at least the rank of Superintendent, appointed by the Commissioner of Police.
(3) The Unit is the sole agency responsible for the investigation of cybercrime offences under this Act and under any other law of Papua New Guinea. The Authority does not perform cybercrime investigation functions.
(4) All cybercrime investigation functions that may arise in the administration of this Act — including the exercise of investigation powers under Part VIII — are performed exclusively by officers of the Unit designated as authorised investigators under Section 71.

64. PROVINCIAL CYBERCRIME INVESTIGATION OFFICES.

(1) The Commissioner of Police must establish a Cybercrime Investigation Office in each Province of Papua New Guinea.
(2) Each Provincial Cybercrime Investigation Office must be operational within 3 years of the commencement of this Part.
(3) Each Provincial Cybercrime Investigation Office must be staffed by at least —
    (a) one officer trained in digital forensics; and
    (b) one officer trained in cybercrime investigation.
(4) Each Provincial Cybercrime Investigation Office must have access to the equipment prescribed for the purposes of digital forensics investigations.

65. FUNCTIONS OF THE UNIT.

The functions of the Unit are to —
    (a) investigate cybercrime offences under this Act and other applicable laws;
    (b) collect, preserve, and analyse digital evidence;
    (c) conduct digital forensics examinations;
    (d) coordinate with the Authority, CERT, and other agencies on cybercrime incidents;
    (e) liaise with international law enforcement agencies on transnational cybercrime;
    (f) refer matters to the National Prosecution Service for prosecution; and
    (g) maintain and develop capacity in cybercrime investigation and digital forensics.

66. QUALIFICATIONS AND TRAINING.

(1) An officer appointed to serve in the Unit must have completed the training program prescribed for cybercrime investigation.
(2) The Commissioner of Police must ensure that officers of the Unit undertake regular continuing professional development in cybercrime investigation and digital forensics.
(3) The Authority must provide training support and technical resources to the Unit.

67. DIGITAL FORENSICS LABORATORY.

(1) The Unit must establish and maintain a Digital Forensics Laboratory equipped to —
    (a) extract, preserve, and analyse data from digital devices;
    (b) conduct network forensics examinations;
    (c) analyse malware and ransomware; and
    (d) prepare forensic reports for use in legal proceedings.
(2) The Digital Forensics Laboratory must meet the standards prescribed by the Authority in consultation with the Unit.

68. COORDINATION WITH THE NATIONAL PROSECUTION SERVICE.

(1) The Unit must maintain a direct liaison relationship with the Office of the Public Prosecutor for the purpose of ensuring the effective prosecution of cybercrime offences.
(2) The Unit and the Office of the Public Prosecutor must jointly develop guidelines on —
    (a) the handling and presentation of digital evidence in court; and
    (b) the preparation of cybercrime prosecution briefs.

69. COOPERATION WITH THE AUTHORITY.

(1) The Unit and the Authority must cooperate in the exercise of their respective functions under this Act.
(2) The Unit may provide technical assistance to the Authority and the Authority may provide technical support to the Unit.

70. RESOURCING OBLIGATIONS.

(1) The National Executive Council must ensure that adequate funding, equipment, and staffing are allocated to the Unit in each annual national budget.
(2) The Commissioner of Police must include a report on the operations and resourcing of the Unit in the annual report of the Royal Papua New Guinea Constabulary.

PART VIII - INVESTIGATION POWERS AND DIGITAL EVIDENCE

71. AUTHORISED INVESTIGATORS.

(1) The Commissioner of Police may designate officers of the Unit as authorised investigators for the purposes of this Part.
(2) An authorised investigator may exercise the powers conferred by this Part for the purpose of investigating an offence under this Act.

72. SEARCH WARRANT — DIGITAL DEVICES.

(1) An authorised investigator may apply to a Magistrate or Judge for a warrant to search premises and seize digital devices.
(2) An application under Subsection (1) must state —
    (a) the grounds for believing that an offence under this Act has been, is being, or is about to be committed;
    (b) the premises to be searched;
    (c) the type of digital devices or data sought; and
    (d) the connection between the devices or data and the suspected offence.
(3) A Magistrate or Judge may issue a warrant if satisfied that there are reasonable grounds for the belief stated in the application.
(4) A warrant issued under this section authorises the authorised investigator to —
    (a) enter and search the specified premises;
    (b) seize any digital device that may contain evidence of the offence;
    (c) extract data from any device found on the premises; and
    (d) copy and retain any data relevant to the suspected offence.

73. PRESERVATION ORDER.

(1) An authorised investigator may apply ex parte to a Magistrate or Judge for an order requiring a person holding data to preserve that data.
(2) A preservation order may require —
    (a) the person to preserve specified data for a period not exceeding 90 days;
    (b) the person not to delete, alter, or disclose the data pending further order; and
    (c) the person to confirm in writing the data preserved and the format of preservation.
(3) A Magistrate or Judge must not issue a preservation order unless satisfied that there are reasonable grounds to believe that the data is relevant to an investigation of an offence under this Act.
(4) A person who fails to comply with a preservation order commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 2 years, or both.

(4) An order under this section must be limited to data reasonably necessary for the investigation. Personal data preserved under this section shall be protected against unauthorised access or use, and any data found to be irrelevant to the investigation shall be deleted or returned as soon as practicable, subject to any contrary court order.

74. PRODUCTION ORDER.

(1) An authorised investigator may apply to a Magistrate or Judge for an order requiring a specified person to produce specified data or documents.
(2) A production order may require —
    (a) an internet service provider to produce traffic data, subscriber information, or content data;
    (b) a financial institution to produce account records or transaction data;
    (c) a social media platform to produce user data, account information, or content; or

(d) any other person to produce data relevant to a cybercrime investigation.

(3) A person who fails to comply with a production order, without reasonable excuse, commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 2 years, or both.

(5) A production order under this section must identify the data sought with reasonable specificity and be confined to data necessary and proportionate for the purpose of the investigation. Personal data obtained pursuant to this section shall be handled, secured, retained and disclosed only in accordance with this Act and the Data Governance and Data Protection Act 2026.

75. LAWFUL INTERCEPTION OF ELECTRONIC COMMUNICATIONS.

(1) An authorised investigator may apply to a Judge of the National Court for an interception warrant authorising the interception of electronic communications.

(2) A Judge may issue an interception warrant only if satisfied that —

(a) there are reasonable grounds to believe that a serious offence under this Act is being, has been, or is about to be committed;

(b) the interception is likely to produce evidence relevant to the offence; and

(c) other investigative methods have been tried and failed, or are unlikely to succeed.

(3) An interception warrant must specify —

(a) the person or account subject to interception;

(b) the type of communications to be intercepted;

(c) the period of interception, not exceeding 60 days; and

(d) conditions on the use of intercepted material.

(5) Interception under this section shall be undertaken only where necessary and proportionate, and any personal data obtained that is not relevant to the offence or threat under investigation shall be isolated and destroyed as soon as practicable. Records of access, use, copying and disclosure of intercepted data shall be maintained.

76. SAFEGUARDS FOR INTERCEPTION.

(1) Intercepted material must be used only for the purpose of the investigation authorised by the interception warrant.

(2) Intercepted material must be destroyed as soon as it is no longer required for the purposes of an investigation or prosecution.

(3) Communications that are subject to legal professional privilege must not be used in evidence.

77. ADMISSIBILITY OF DIGITAL EVIDENCE.

(1) In this Part, "digital evidence" means any information stored, generated, processed, or transmitted in digital form that is relevant to a legal proceeding, and includes data, records, messages, logs, and metadata.

(2) Digital evidence is admissible in any proceeding before a court or tribunal in Papua New Guinea if —

(a) it is relevant to a matter in question; and

(b) it is authenticated in accordance with Section 78.

(3) Digital evidence is not inadmissible merely because it is a copy, provided the copy was made and maintained in accordance with the prescribed standards.

78. AUTHENTICATION OF DIGITAL RECORDS.

(1) A digital record may be authenticated by —

(a) a certificate of a digital forensic analyst under Section 80;

(b) evidence of the system from which the record was produced;

(c) metadata demonstrating the origin and integrity of the record; or

(d) any other means prescribed by regulation.

79. CHAIN OF CUSTODY.

(1) An authorised investigator who seizes a digital device or extracts digital data must —
- (a) maintain a written chain of custody record from the time of seizure or extraction;
- (b) record each person who has had possession of or access to the device or data;
- (c) seal the device or store the data in accordance with the prescribed forensic standards; and
- (d) ensure that the device or data is not altered after seizure.

80. CERTIFICATE OF DIGITAL FORENSIC ANALYST.

(1) A certificate signed by a qualified digital forensic analyst certifying as to —
- (a) the method used to extract, copy, or analyse digital evidence;
- (b) the integrity of the digital evidence; and
- (c) any other matter relevant to the admissibility or interpretation of the evidence,

is admissible in any proceeding as evidence of the matters stated in it, unless the contrary is proved.

(2) A party who wishes to challenge a certificate under Subsection (1) must give notice of that intention at least 14 days before the relevant hearing.

81. EXTRATERRITORIAL INVESTIGATION.

Where an investigation under this Part requires access to data or devices located outside Papua New Guinea, the Unit may request assistance through the mutual legal assistance mechanisms in Part XIII.

82. OBSTRUCTION OF INVESTIGATION.

(1) A person must not obstruct, hinder, or interfere with an authorised investigator in the exercise of powers under this Part.

Penalty: A fine not exceeding K50,000 or imprisonment for a term not exceeding 1 year, or both.

83. PROTECTION OF PRIVILEGED MATERIAL.

Nothing in this Part authorises the seizure, production, or interception of material that is subject to legal professional privilege.

84. AMENDMENT OF EVIDENCE ACT 1975.

The Evidence Act 1975 is amended in accordance with Schedule 4 to give effect to the admissibility provisions in this Part.

PART IX - CYBERCRIME OFFENCES AND PENALTIES

85. UNAUTHORISED ACCESS TO A COMPUTER SYSTEM.

(1) A person who intentionally and without authorisation accesses the whole or part of a computer system commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 5 years, or both.

(2) It is not a defence that the person did not know the system was that of a particular victim.

86. UNAUTHORISED ACCESS — AGGRAVATED.

A person who commits an offence under Section 85 commits an aggravated offence if the offence was committed —

(a) against a CII facility or system;
(b) against the computer systems of a financial institution;
(c) against the computer systems of a government body or national security agency;
(d) with intent to steal, modify, or destroy data; or
(e) by means of malware.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

87. DATA INTERFERENCE.

A person who, without authorisation, intentionally damages, deletes, deteriorates, alters, or suppresses data on a computer system commits an offence.

Penalty: A fine not exceeding K200,000 or imprisonment for a term not exceeding 7 years, or both.

88. SYSTEM INTERFERENCE.

(1) A person who, without authorisation, intentionally hinders or interrupts the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing data commits an offence.

Penalty: A fine not exceeding K300,000 or imprisonment for a term not exceeding 10 years, or both.

(2) An offence under Subsection (1) committed against CII is an aggravated offence.

Penalty: A fine not exceeding K1,000,000 or imprisonment for a term not exceeding 25 years, or both.

89. RANSOMWARE AND MALWARE.

(1) A person who intentionally —

(a) produces, distributes, or possesses malware for use in committing an offence; or
(b) deploys ransomware against a computer system,

commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

(2) An offence under Subsection (1)(b) committed against CII or a health system is an aggravated offence.

Penalty: A fine not exceeding K1,000,000 or imprisonment for a term not exceeding 25 years, or both.

90. CYBER EXTORTION.

A person who, using a computer system, threatens to —

(a) damage, destroy, or deny access to data or a computer system;
(b) disclose sensitive, private, or intimate information; or
(c) expose or publicise harmful material relating to the victim,

with intent to extort money, property, or any other advantage commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

91. DENIAL-OF-SERVICE ATTACKS.

A person who, without authorisation, intentionally hinders access to a computer system by sending, directing, or facilitating the transmission of an excessive volume of data or requests commits an offence.

Penalty: A fine not exceeding K300,000 or imprisonment for a term not exceeding 10 years, or both.

92. UNLAWFUL INTERCEPTION OF COMMUNICATIONS.

A person who, without lawful authority, intentionally intercepts electronic communications while they are being transmitted commits an offence.

Penalty: A fine not exceeding K200,000 or imprisonment for a term not exceeding 7 years, or both.

93. DATA ESPIONAGE AND INTERFERENCE WITH STATE SECRETS.

A person who, without authorisation, accesses, copies, transmits, or discloses —

(a) classified government information;
(b) defence or national security data; or
(c) information relating to the intelligence activities of the State,

commits an offence.

Penalty: A fine not exceeding K1,000,000 or imprisonment for a term not exceeding 25 years, or both.

94. INTERFERENCE WITH CRITICAL INFRASTRUCTURE.

A person who, with intent to endanger public safety, disrupt essential services, or damage national security, causes a major disruption to critical information infrastructure commits an offence.

Penalty: Imprisonment for life.

95. AI-ENABLED ATTACKS AND SYNTHETIC MEDIA FRAUD.

A person who uses an AI system to create a deepfake for the purpose of —

(a) defrauding or deceiving another person;
(b) obtaining a financial advantage by deception;
(c) damaging the reputation of another person; or
(d) creating child sexual exploitation material,

commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

96. CRYPTOCURRENCY AND DIGITAL ASSET FRAUD.

A person who, using a computer system, dishonestly —

(a) operates a fraudulent cryptocurrency investment scheme;
(b) manipulates the value of a digital asset; or
(c) receives or converts digital assets knowing them to be proceeds of cybercrime,

commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 15 years, or both.

97. ONLINE HARASSMENT AND CYBERSTALKING.

A person who, using a computer system, repeatedly communicates with or about another person in a manner that causes the other person fear, distress, or alarm commits an offence.

Penalty: A fine not exceeding K50,000 or imprisonment for a term not exceeding 3 years, or both.

98. DISINFORMATION CAUSING PUBLIC HARM.

A person who intentionally publishes or distributes information that the person knows to be false, using a computer system, in circumstances likely to cause —

(a) public panic or disorder;
(b) harm to an identifiable group; or
(c) serious reputational harm to a public institution,

commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 3 years, or both.

99. MISUSE OF ILLEGAL DEVICES.

A person who intentionally produces, sells, procures for use, imports, or distributes —

(a) a device designed primarily to commit offences under this Part; or
(b) a computer program designed primarily to commit offences under this Part,

with the intent that it be used to commit an offence under this Act, commits an offence.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 5 years, or both.

100. FAILURE TO COMPLY WITH MANDATORY REPORTING.

A person or entity required to report a cybersecurity incident under this Act who fails to do so within the time prescribed commits an offence.

Penalty: A fine not exceeding K50,000.

101. CORPORATE LIABILITY.

(1) Where a body corporate commits an offence under this Part, each director, manager, or officer who authorised, permitted, or failed to prevent the commission of the offence is taken to have committed the offence and is liable to the penalty prescribed for an individual.

(2) It is a defence for a person charged under Subsection (1) to prove that he or she took all reasonable steps to prevent the commission of the offence.

102. ATTEMPT AND CONSPIRACY.

(1) A person who attempts to commit, or conspires to commit, an offence under this Part commits an offence and is liable to the penalty for the substantive offence.

PART X
PLATFORM AND ICT SERVICE PROVIDER OBLIGATIONS

103. REGISTRATION OF PLATFORMS.

(1) A social media platform or ICT service provider operating in or accessible from Papua New Guinea with more than 10,000 active users in Papua New Guinea must register with the Authority in the prescribed manner.
(2) Registration must be renewed annually.

104. CONTENT REMOVAL OBLIGATIONS.

A registered platform must remove content that —
(a) constitutes child sexual exploitation material;
(b) facilitates cybercrime;
(c) constitutes an offence under this Act or any other law; or
(d) poses an imminent threat to public safety,
within 24 hours of becoming aware of it or receiving a notice from the Authority.

105. TAKEDOWN NOTICES.

(1) The Authority or the Commissioner may issue a written takedown notice to a platform requiring the removal of specified content.
(2) A platform that fails to comply with a takedown notice within 24 hours without reasonable excuse commits an offence.

Penalty: A fine not exceeding K500,000.

106. DATA RETENTION OBLIGATIONS.

(1) A registered platform or ICT service provider must retain only those categories of subscriber registration information, traffic data and user identification data expressly prescribed by law and strictly necessary for cybersecurity, lawful investigation or compliance purposes, for a period not exceeding 24 months. Data retained under this section must be secured, access-controlled, used only for lawful purposes, and securely deleted or irreversibly anonymised upon expiry of the retention period.
(2) Data retained under Subsection (1) must be produced to an authorised investigator when required by a production order under Section 74.

107. REPORTING DUTIES OF PLATFORMS.

(1) A registered platform must report to the Authority —
(a) any significant cybersecurity incident affecting its systems within 48 hours; and
(b) any case of child sexual exploitation material discovered on its platform within 24 hours.

108. LIMITATION OF LIABILITY.

A platform is not criminally or civilly liable for content posted by a user unless the platform —
(a) knew of the content and failed to remove it within the required time;
(b) was notified of the content and failed to act; or
(c) created, generated, or materially contributed to the content.

109. OFFENCE — NON-COMPLIANCE BY ICT SERVICE PROVIDER.

A registered platform or ICT service provider that fails to comply with a requirement under this Part without reasonable excuse commits an offence.

Penalty: A fine not exceeding K1,000,000.

110. COOPERATION WITH INVESTIGATION.

A registered platform or ICT service provider must —'

(a) cooperate fully with any investigation conducted by the Unit or the Authority;
(b) designate a contact officer in Papua New Guinea for law enforcement liaison; and
(c) maintain technical capability to respond to lawful production orders within 48 hours.

PART XI - INCIDENT REPORTING AND EMERGENCY POWERS

111. MANDATORY INCIDENT REPORTING.

(4) Where a cybersecurity incident reported under this section involves personal data, compliance with this section does not remove or limit the obligation to notify a personal data breach under the Data Governance and Data Protection Act 2026. A report under this section may satisfy that obligation only if it contains the information required under that Act.

(5) Where a reported cybersecurity incident is likely to result in a high risk to the rights or freedoms of affected individuals, the responsible entity must notify affected data subjects without undue delay in accordance with Section 64 of the Data Governance and Data Protection Act 2026, unless an exemption under that Act or a lawful investigative restriction applies.

(1) A person or entity that manages a computer system that suffers a cybersecurity incident must notify the Authority in the prescribed manner within —

(a) 24 hours, in the case of a CII operator or financial institution; or

(b) 72 hours, in the case of any other entity.

(2) A notification under Subsection (1) must include the information prescribed by the Authority.

112. CYBERSECURITY RESPONSE CENTRE.

The Authority must operate a Cybersecurity Response Centre to —

(a) receive and triage incident reports;

(b) coordinate national cybersecurity response;

(c) issue public threat advisories and bulletins;

(d) provide technical assistance to entities affected by incidents; and

(e) maintain a national cybersecurity incident database.

113. DECLARATION OF CYBERSECURITY EMERGENCY.

The Minister may, by notice published in the National Gazette, declare a cybersecurity emergency if the Minister is satisfied, on the advice of the Authority, that —

(a) a cybersecurity incident has occurred or is imminent;

(b) the incident threatens national security, essential services, or public safety; and

(c) existing powers under this Act are insufficient to address the threat.

114. EMERGENCY DIRECTIONS.

(1) During a cybersecurity emergency, the Minister may issue written directions to —

(a) any person or entity to isolate, disconnect, or shut down specified computer systems;

(b) an ICT service provider to restrict access to specified services or content;

(c) a CII operator to implement specified emergency cybersecurity measures; and

(d) any government agency to take specified cybersecurity response actions.

(2) A person who fails to comply with an emergency direction without reasonable excuse commits an offence.

Penalty: A fine not exceeding K500,000 or imprisonment for a term not exceeding 10 years, or both.

115. DURATION OF EMERGENCY.

(1) A cybersecurity emergency declaration remains in force for a period not exceeding 30 days.

(2) The Minister may, by further notice published in the National Gazette, renew a declaration for a period not exceeding 30 days, but only if —

(a) the National Parliament passes a resolution approving the renewal; or

(b) the Parliament is not sitting and urgency prevents convening it.

116. PARLIAMENTARY OVERSIGHT OF EMERGENCY.

(1) The Minister must notify the Parliament of a cybersecurity emergency declaration within 7 days of its making.
(2) The Parliament may, by resolution, revoke a cybersecurity emergency declaration at any time.

117. JUDICIAL REVIEW PRESERVED.

Nothing in this Part limits the right of a person affected by a direction under Section 114 to seek judicial review of that direction.

118. COMPENSATION.

A person who suffers loss or damage as a result of a direction under Section 114 that is found to have been unreasonable or disproportionate is entitled to compensation from the State.

PART XII - LICENSING AND REGULATION OF CYBERSECURITY SERVICES

119. LICENCE REQUIRED.

(1) A person must not provide cybersecurity services, including auditing, penetration testing, digital forensics, or managed security services, unless that person holds a licence issued under this Part.

Penalty: A fine not exceeding K100,000 or imprisonment for a term not exceeding 2 years, or both.

(2) Subsection (1) does not apply to an employee performing cybersecurity functions within their employing organisation.

120. APPLICATION FOR LICENCE.

(1) A person may apply to the Authority for a licence to provide cybersecurity services.
(2) An application must —
- (a) be in the approved form;
- (b) be accompanied by the prescribed fee; and
- (c) include evidence of the applicant's qualifications and relevant experience.

121. GRANT OR REFUSAL OF LICENCE.

(1) The Authority must grant a licence if satisfied that the applicant —
- (a) has the qualifications and experience required by the regulations;
- (b) is of good character; and
- (c) has adequate capacity to provide the cybersecurity services for which the licence is sought.

(2) The Authority must refuse a licence if not satisfied under Subsection (1), and must give the applicant written notice of the refusal and the reasons, and the right to appeal under Section 141.

122. DURATION AND RENEWAL.

(1) A licence remains in force for 2 years unless earlier suspended or cancelled.
(2) A licensee may apply for renewal within 60 days before the licence expires.

123. SUSPENSION AND CANCELLATION.

(1) The Authority may suspend or cancel a licence if the licensee —
- (a) ceases to meet the requirements for the grant of a licence;
- (b) has committed an offence under this Act or any other relevant law;
- (c) has engaged in conduct that is prejudicial to cybersecurity in Papua New Guinea; or
- (d) fails to comply with the conditions of the licence.

(2) The Authority must give the licensee reasonable notice and an opportunity to be heard before suspending or cancelling a licence.

124. ACCREDITATION OF CYBERSECURITY PROFESSIONALS.

(1) The Authority must establish and maintain a register of accredited cybersecurity professionals.
(2) A person may apply to the Authority for accreditation as a cybersecurity professional.
(3) The Authority must prescribe the qualifications, experience, and continuing professional development requirements for accreditation.

PART XIII - INTERNATIONAL COOPERATION

125. INTERNATIONAL COOPERATION — GENERAL.

(1) The Authority may cooperate with foreign governments, international organisations, and cybersecurity agencies in —
  (a) sharing cybersecurity threat intelligence;
  (b) coordinating responses to transnational cybercrime;
  (c) providing and receiving technical assistance; and
  (d) developing harmonised cybersecurity standards and policies.

(2) Cooperation under this section must be consistent with the laws and applicable treaties of Papua New Guinea.

126. MUTUAL LEGAL ASSISTANCE.

(1) Papua New Guinea may provide mutual legal assistance in cybercrime investigations to a foreign country —
  (a) under any bilateral or multilateral treaty or arrangement; or
  (b) on the basis of reciprocity, subject to the approval of the Attorney-General.

(2) A request for mutual legal assistance from a foreign country must be made through the diplomatic channel or through the channels established under an applicable treaty.

127. CROSS-BORDER DIGITAL EVIDENCE.

Papua New Guinea may provide or request assistance in obtaining digital evidence located in another jurisdiction in accordance with —
  (a) an applicable mutual legal assistance treaty;
  (b) the Mutual Assistance in Criminal Matters Act; or
  (c) the Budapest Convention, upon accession.

127A. Where cooperation, mutual legal assistance or evidence-sharing under this Part involves personal data, any disclosure or transfer shall comply with the cross-border transfer requirements of the Data Governance and Data Protection Act 2026, unless otherwise authorised by a court order, a mutual legal assistance law, or another written law, and only to the extent necessary and proportionate for the relevant proceeding or cybersecurity purpose.

128. CERT-TO-CERT COOPERATION.

The CERT may cooperate directly with the computer emergency response teams of other countries and with international CERT networks for the purpose of —
  (a) sharing threat intelligence and incident data; and
  (b) coordinating technical responses to cross-border cybersecurity incidents.

129. ACCESSION TO BUDAPEST CONVENTION.

(1) The Government of Papua New Guinea, having been invited to accede to the Budapest Convention in October 2024, must take all steps necessary to give effect to accession within 2 years of the commencement of this Part.

(2) Upon accession, the Authority must ensure that the offence provisions of this Act are interpreted consistently with the Budapest Convention.

130. DESIGNATION OF CONTACT POINT.

(1) The Authority is designated as the national contact point for the purposes of international cybercrime cooperation.

(2) The Authority must maintain the capacity to respond to international cybercrime cooperation requests on a 24-hours-a-day, 7-days-a-week basis.

PART XIV - CAPACITY BUILDING AND PUBLIC AWARENESS

131. NATIONAL CYBERSECURITY SKILLS DEVELOPMENT.

(1) The Authority must, in collaboration with the Department of Higher Education, Research, Science and Technology and NICTA, develop and implement a national cybersecurity skills development program.

(2) The program must provide for —

(a) scholarships for cybersecurity studies;
(b) accredited professional training for government and private sector employees;
(c) specialist training for the Unit and other law enforcement agencies; and
(d) pathways for Papua New Guineans to become accredited cybersecurity professionals.

132. CURRICULUM INTEGRATION.

The Authority must work with the Department of Education and relevant institutions to integrate cybersecurity education and cyber safety awareness into —

(a) the national primary and secondary school curriculum; and
(b) vocational and technical training programs.

133. PUBLIC AWARENESS CAMPAIGNS.

(1) The Authority must conduct ongoing public awareness campaigns on —

(a) cyber hygiene and safe online behaviour;
(b) child online safety and the risks of social media;
(c) financial cybercrime and how to identify phishing and scams;
(d) how to report cybercrime and cybersecurity incidents; and
(e) the rights and responsibilities of citizens in cyberspace.

134. CYBERSECURITY INNOVATION FUND.

The Minister may establish a Cybersecurity Innovation Fund to support —

(a) local research into cybersecurity technologies;
(b) development of indigenous digital security solutions;
(c) pilot cybersecurity projects; and
(d) academic and industry cybersecurity partnerships.

135. RESEARCH AND DEVELOPMENT PARTNERSHIPS.

The Authority may enter into partnerships with academic institutions, technology companies, and international cybersecurity organisations for the purpose of research and development in cybersecurity.

136. PACIFIC REGIONAL COOPERATION.

The Authority must actively participate in regional cybersecurity cooperation through —

(a) the Pacific Cyber Security Operational Network (PaCSON);
(b) the Global Forum on Cyber Expertise (GFCE);
(c) the Pacific Islands Forum cybersecurity initiatives; and
(d) any other regional or international cybersecurity body the Minister approves.

PART XV - MISCELLANEOUS

137. PROTECTION OF PERSONAL DATA.

In carrying out functions under this Act, the Authority and every person exercising powers or performing duties under this Act must handle personal data in accordance with the Data Governance and Data Protection Act 2026 and must apply the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, integrity, confidentiality, accountability and data sovereignty.

138. PROTECTION FROM LIABILITY.

A member of the Board, the Chief Executive Officer, or an officer of the Authority is not personally liable for anything done or omitted in good faith in the performance of a function or the exercise of a power under this Act.

139. DELEGATION.

(1) The Authority may, by written instrument, delegate any of its powers or functions under this Act to a person or class of persons, other than this power of delegation.
(2) A delegation does not prevent the Authority from exercising the delegated power or function.

140. INFRINGEMENT NOTICES.

(1) An authorised officer who has reason to believe that a person has committed an offence against this Act that is prescribed as an infringement offence may issue a written infringement notice to that person.
(2) An infringement notice must state —
    (a) the alleged offence;
    (b) the infringement penalty, being one-tenth of the maximum penalty for the offence;
    (c) the period for payment; and
    (d) that if the penalty is paid, no further action will be taken.

141. APPEALS.

(1) A person aggrieved by a decision of the Authority or the Commissioner under this Act may appeal to the National Court against the decision.
(2) An appeal must be lodged within 30 days after the date of the decision.

142. REVIEW OF ACT.

(1) The Department, in consultation with the Authority, must review the operation and effectiveness of this Act every 3 years after commencement.
(2) The Minister must table a report on each review in the Parliament within 30 days of its completion.

143. RELATIONSHIP WITH OTHER LAWS.

(1) This Act is in addition to and does not limit the Cybercrime Code Act 2016, the National Information and Communications Technology Act 2009, the Lukautim Pikinini Act 2015, or any other Act.
(2) Where there is an inconsistency between this Act and the Cybercrime Code Act 2016, this Act prevails to the extent of the inconsistency.
(3) This Act shall be read together with the Data Governance and Data Protection Act 2026. To the extent that any act, omission, disclosure, retention, transfer or other processing under this Act involves personal data, the Data Governance and Data Protection Act 2026 applies as the

governing law on personal data protection, except where this Act expressly provides a more specific cybersecurity obligation that is necessary, proportionate and lawful.

144. TRANSITIONAL PROVISIONS.

(1) NICTA is, on and from the commencement of Part II, deemed to be the National Cybersecurity Authority for the purposes of this Act, in accordance with Section 7.
(2) NICTA must, within 3 months of the commencement of Part II —
    (a) establish a dedicated Cybersecurity Division within its organisational structure for the performance of its functions under this Act; and
    (b) designate a Cybersecurity Division Director who will be responsible for the day-to-day administration of NICTA's functions under this Act and who will serve as the primary point of contact for the Minister and for the Cybercrime Investigation Unit.
(3) The National Cybersecurity Centre established within NICTA with the support of the Australian Government in 2018 continues to operate on and from the commencement of this Act as the Cybersecurity Operations Centre under Section 31, until NICTA establishes a replacement Centre.
(4) The Papua New Guinea Computer Emergency Response Team (PNGCERT) operating within NICTA at the date of commencement continues to operate as the CERT established by Section 28 of this Act.
(5) The Cybercrime Investigation Unit of the Royal Papua New Guinea Constabulary, including the Cybercrime Unit operating at the date of commencement, is taken to be established under Section 63 of this Act, and may continue operating without interruption.
(6) Any agreement, arrangement, cooperation framework, or policy in force immediately before the commencement of this Act that relates to cybersecurity or cybercrime continues in force on and after commencement and is taken to have been made under this Act.
(7) Where the National Executive Council makes a decision under Section 8 to establish a separate National Cybersecurity Authority —
    (a) the Minister must publish a notice in the National Gazette within 30 days of the NEC decision;
    (b) NICTA's deemed status as the Authority under Section 7 ceases on the date specified in that notice; and
(c) NICTA and the separate Authority must cooperate to ensure an orderly transition of functions, assets, staff, and agreements in accordance with Section 9.

145. SAVINGS.

Nothing in this Act limits the liability of a person for an offence committed before the commencement of this Act under any law in force at the time of the commission of the offence.

146. REGULATIONS.

(1) The Head of State, acting on advice, may make regulations not inconsistent with this Act prescribing all matters required or permitted to be prescribed, or necessary or convenient to be prescribed, for carrying out or giving effect to this Act.
(2) Without limiting Subsection (1), regulations may prescribe —
    (a) forms to be used under this Act;
    (b) fees and charges payable under this Act;
    (c) standards for digital forensics;
    (d) cybersecurity standards for CII operators and financial institutions;
    (e) minimum qualifications for cybersecurity professionals; and
    (f) penalties not exceeding K50,000 for offences against the regulations.

147. CONSEQUENTIAL AMENDMENTS.

The Acts set out in Schedule 4 are amended as specified in that Schedule.

148. MISUSE OF PERSONAL DATA OBTAINED UNDER THIS ACT.

(1) A person who, without lawful authority, uses, discloses, retains, copies, sells, publishes or otherwise deals with personal data obtained under this Act for a purpose not authorised by this Act or any other written law commits an offence.

(2) The Authority may also impose an administrative penalty where appropriate, without limiting any remedy or sanction under the Data Governance and Data Protection Act 2026.

SCHEDULE 1

DESIGNATED CRITICAL INFORMATION INFRASTRUCTURE SECTORS

(Section 31(3))

PART A — DESIGNATED SECTORS

Sector	Description
1. Banking and Finance	Banks, insurance companies, payment service providers, stock exchange, and all entities licensed by the Bank of Papua New Guinea
2. Telecommunications	All licensed telecommunications network operators, internet service providers, and mobile network operators
3. Energy	Electricity generation, transmission, and distribution; petroleum and gas pipelines; PNG Power Limited
4. Transport	Air traffic management; Jacksons and all international airports; Port Moresby and major seaports; National road traffic management
5. Water and Sanitation	Eda Ranu and all urban water utilities; sewage treatment and waste management systems
6. Health	All public hospital networks; National Department of Health information systems; National Health Information System
7. Government	Department of Finance IFMS; Department of Personnel Management payroll systems; National Parliament; National Court; Office of the Electoral Commission
8. Extractive Industries	ExxonMobil PNG, Oil Search, Barrick Niugini, PNG LNG — operational technology and SCADA systems for pipeline, processing, and mine management
9. Education	University of Papua New Guinea, PNG University of Technology, Divine Word University — and all tertiary institution administrative systems

PART B — HIGH-RISK SOCIAL MEDIA PLATFORMS

For the purposes of Section 48, the following are declared to be high-risk social media platforms to which Section 49 applies:

Facebook; Instagram; TikTok; X (formerly Twitter); Snapchat; YouTube; Reddit; Threads; WhatsApp (public groups); Telegram (public channels); Bigo Live; and any other platform added by the Commissioner by notice in the National Gazette.

SCHEDULE 2

PENALTY TABLES

(Part IX)

S.	Offence	Max Fine	Max Imprisonment	Mode
83	Unauthorised access	K100,000	5 years	Indictable
84	Unauthorised access — aggravated	K500,000	15 years	Indictable
85	Data interference	K200,000	7 years	Indictable
86	System interference	K300,000	10 years	Indictable
86	System interference — CII	K1,000,000	25 years	Indictable
87	Ransomware/malware	K500,000	15 years	Indictable
87	Ransomware — CII/health	K1,000,000	25 years	Indictable
88	Cyber extortion	K500,000	15 years	Indictable
89	Denial-of-service	K300,000	10 years	Indictable
90	Unlawful interception	K200,000	7 years	Indictable

91	Data espionage	K1,000,000	25 years	Indictable
92	CII interference	—	Life	Indictable
93	AI/deepfake fraud	K500,000	15 years	Indictable
94	Cryptocurrency fraud	K500,000	15 years	Indictable
95	Cyber harassment	K50,000	3 years	Summary
96	Disinformation	K100,000	3 years	Summary
97	Illegal devices	K100,000	5 years	Indictable
53	Grooming	—	15 years	Indictable
54	CSEM	—	Life	Indictable
55	Cyberbullying (child)	K100,000	3 years	Summary/Indictable
56	Non-consensual intimate images	K200,000	5 years	Indictable

SCHEDULE 3

BUDAPEST CONVENTION OFFENCE ALIGNMENT

(Section 129)

The following table sets out the alignment between offences in this Act and the offences required by the Budapest Convention on Cybercrime (ETS No. 185).

Budapest Convention Article	This Act	Notes
Art. 2 — Illegal access	Section 85 and 84	Fully implemented with aggravated offence
Art. 3 — Illegal interception	Section 92	Fully implemented
Art. 4 — Data interference	Section 87	Fully implemented
Art. 5 — System interference	Section 88	Fully implemented with aggravated offence for CII
Art. 6 — Misuse of devices	Section 99	Fully implemented
Art. 7 — Computer-related forgery	Section 44	Implemented through electronic fraud provisions
Art. 8 — Computer-related fraud	Sections 40, 41, 42	Fully implemented with enhanced financial sector provisions
Art. 9 — Child pornography	Section 56	Implemented; broader than Convention — includes AI-generated CSEM
Art. 29 — Expedited preservation	Section 73	Fully implemented
Art. 30 — Partial disclosure	Section 73(2)	Implemented in preservation order provisions
Art. 31 — Production order	Section 74	Fully implemented
Art. 32 — Access to stored data	Sections 70 and 72	Implemented via search warrant and production order
Art. 33 — Real-time collection	Section 75	Implemented via interception warrant
Art. 34 — Interception	Sections 73 and 74	Fully implemented with safeguards

SCHEDULE 4

CONSEQUENTIAL AMENDMENTS AND PRESCRIBED FORMS

PART A — AMENDMENT OF EVIDENCE ACT 1975

After Section 52 of the Evidence Act 1975, insert the following:

'50A. Digital evidence.

(1) A digital record produced in the ordinary course of a computer system's operation is admissible as evidence of the facts it records.

(2) A copy of a digital record is admissible to the same extent as the original if the copy was made and maintained in accordance with the standards prescribed under the Cybersecurity Act 2026.
(3) A certificate of a digital forensic analyst under Section 80 of the Cybersecurity Act 2026 is admissible as evidence of the matters certified.'

PART B — PRESCRIBED FORMS

The following forms are prescribed for the purposes of this Act:

Form 1 — Mandatory Incident Report (Section 111)
Form 2 — Application for Cybersecurity Service Provider Licence (Section 120)
Form 3 — CII Incident Report (Section 35)
Form 4 — Infringement Notice (Section 140)
Form 5 — Application for Preservation Order (Section 73)
Form 6 — Application for Production Order (Section 74)