REPUBLIC OF VANUATU

BILL FOR THE DIGITAL TRANSFORMATION ACT NO. OF 2025

Explanatory Note

The Government of Vanuatu aims to establish a comprehensive legal framework for advancing digital development, e-Governance, and innovation in Vanuatu. It outlines the roles, responsibilities, and authority of the Department of Communications and Digital Transformation (DCDT), ensuring they align with the National Sustainable Development Plan (NSDP 2016–2030), the Digital Government Master Plan, and the Cybersecurity Strategy 2030 and related policies.

The proposed bill reflects the Government's commitment to modernizing public service delivery, improving national ICT governance, and creating an environment supportive of inclusive digital transformation and growing Vanuatu's digital economy.

The bill aims to consolidate existing functions and to introduce new legal mechanisms in order to support innovation in terms of e-governance, cybersecurity, digital public infrastructures, digital inclusion and the overall digital economy. It grants the Department of Communications and Digital Transformation powers and responsibilities to coordinate national policies, oversee digital infrastructure, and regulate ICT service providers.

The key features of the Bill are:

1. To establish a clear legal and policy mandate for digital transformation

- Defining digital transformation and clarifying the functions, and powers of the Department and the Director in leading Vanuatu's digital agenda.
- To establish a clear legal and policy framework that guides the Government and the private sector in implementing, coordinating, and regulating digital transformation initiatives across all sectors of society.

2. To establish the National Digital Transformation Steering Committee

- Defining the functions and powers of the Committee

3. To regulate ICT activities through a permit system

- Introducing permits for ICT service providers, software developers, hardware repairers, and digital media platforms, with provisions for suspension and cancellation.

4. To enhance compliance and enforcement

- Providing offences, penalties, and enforcement mechanisms to ensure the lawful operation of ICT activities, including the appointment of enforcement officers with inspection and seizure powers.

5. To support interoperability, accountability, and innovation

- To ensure interoperability, cybersecurity, and data privacy standards are adopted throughout the digital transformation process.
- Requiring annual reports, strengthening coordination with statutory bodies and enterprises, and promoting partnerships that encourage digital entrepreneurship, e-commerce, and rural connectivity.

This Bill will establish a comprehensive legal framework to advance Vanuatu's future in digital technologies and digital transformation. It ensures that innovation is aligned with safeguards for cybersecurity, data security, online safety, and citizens' rights, thus supporting the development of a secure, inclusive, and resilient digital society.

Prime Minister

REPUBLIC OF VANUATU

BILL FOR THE DIGITAL TRANSFORMATION ACT NO. OF 2025

Arrangement of Sections

REPUBLIC OF VANUATU

BILL FOR THE DIGITAL TRANSFORMATION ACT NO. OF 2025

An Act to provide for digital transformation and other related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY MATTERS

1 Interpretation

In this Act, unless a contrary intention appears:

Committee means the National Digital Transformation Steering Committee established under section 8;

communication means exchanging information through electronic devices for the transfer of data, text, images, sounds, signs, signals, writing or intelligence of any nature transmitted in whole or in part by electronic means;

cyber security incident means any event that may, without lawful authority:

(a) threaten or potentially jeopardizes, the confidentiality, integrity or availability of a network, an information system or the information that a system processes, stores, or communicates; or

(b) constitutes a violation or imminent threat of violation of security policy, security procedures, or acceptable use policies;

data means

(a) any valuable assets that represent online and offline information integrated and align across platforms to drive informed decision -making, optimize operations, and create personalize customer experiences; and

(b) any representation of facts, concepts or information in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

Department means the Department of Communications and Digital Transformation;

Director means the Director of the Department of Communications and Digital Transformation;

Director General means the Director General responsible of the Ministry responsible for Communications and Digital Transformation;

digital government official engagement means government led initiative that engage government officials in governance processes through digital means, including digital literacy, electronic participation, and consultation platforms;

digital transformation means the process of utilizing and integrating digital technologies and solutions, across all organizational or business areas, leading to fundamental changes in operational methods and value delivery, to customers that encompasses not only the adoption of digital tools, but also entails cultural and operational transitions, aimed at enhancing efficiency, fostering innovation, and satisfying customer requirements;

ICT means Information, Communications and Technology;

ICT services mean:

(a) a digital and data service that includes cloud storage, data analytics, database management, and digital platforms; and

(b) a hardware service that includes the provision of IT equipment and devices, often as part of Hardware as a Service models; and

(c) a software service that includes the application deployment, maintenance, software updates, and patching; and

(d) a technical support that includes the troubleshooting, maintenance, upgrades, and direct IT support; and

(e) a managed service that includes outsourced network, security, or system administration managed by third-party vendors; and

(f) a communication service that includes telecommunication, web portals, and unified communications platforms; and

(g) an infrastructure service that includes data center, network management, hosting, and facilities management; and

(h) a commercial multimedia streaming service; and

(i) a consultancy service that includes IT advisory, system design, and implementation planning; and

(j) artificial intelligence (AI) and AI-related data services; and

(k) hardware and software maintenance; and

(l) cybersecurity governance, risk and compliance services; and

(m) security operation center services;

ICT service provider means an ICT service permit holder that provides any or all of the services listed under the definition of ICT services;

Minister means the Minister responsible for digital transformation;

telecommunication has the same meaning as set out under section 2 of the Telecommunications, Radiocommunication and Broadcasting Regulation Act No. 30 of 2009.

PART 2 ADMINISTRATION

Division 1 Administration

2 Director

(1) The Director is responsible for the day-to-day management and administration of this Act.

(2) The Director must advise and assist the Minister and the Director General in matters relating to the Department as required under this Act.

Division 2 Functions and powers of the Department

3 Functions of the Department

The Department has the following functions:

(a) to formulate and enforce national policies, strategies, and plans for digital transformation; and

(b) to coordinate, and ensure coherence of ICT initiatives across all ministries, departments, and public agencies; and

(c) to act as the central policy and compliance agency responsible for the national digital transformation agenda; and

(d) to assess, arrange for audit, and certify all ICT systems across government for compliance with approved technical and security standards; and

(e) to investigate, and oversee implementation of digital transformation across all public sector, including the management of digital and cyber threats; and

(f) to review and approve all ICT project designs, procurements, and investments, and to issue a Certificate of Compliance (CoC) before funding, procurement, or implementation may proceed; and

(g) to ensure compliance with interoperability standards and national infrastructures such as the Government Broadband Network (GBN), Data Centers, and the .gov.vu domain; and

(h) to develop and enforce national ICT standards, data governance, cybersecurity, and Artificial Intelligence (AI) frameworks; and

(i) to ensure coherence, synergy, and interoperability across all ICT systems, platforms, and digital services implemented by different ministries and government entities, preventing duplication of effort, and investment; and

(j) to oversee the implementation of the Digital Transformation Initiatives to implement the Digital Transformation Masterplan; and

(k) to coordinate inter-agency cooperation and partnerships with key multi-stakeholders; and

(l) to promote digital inclusion, universal services, and innovation; and

(m) to oversee and direct all public sector ICT operations, and may formulate in writing guidelines and issue directives in relation to significant matters to be complied with by government ministries, departments, agencies, and statutory bodies; and

(n) to provide strategic oversight, coordination, and guidance over all national ICT, digital transformation, and Artificial Intelligence (AI) initiatives within the public sector; and

(o) to promote research, development, and responsible adoption of emerging digital technologies, including AI, data analytics, automation, and innovation frameworks; and

(p) to promote, monitor, and report on digital inclusion initiatives at national, rural, and community levels relating to connectivity, digital skills, literacy, and civil service engagement; and

(q) to develop and enforce ICT standards, protocols, and data governance frameworks across the public sector; and

(r) to collaborate with higher education and research institutions, and public private partnerships to support local innovation and sustainable digital growth; and

(s) to review and update national policies and plans regularly to reflect emerging technology trends and implementation performance, including provision for independent review; and

(t) to carry out such other functions as may be conferred on the Department under this Act or any other Act.

4 Powers of the Department

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

(2) Without limiting the generality of subsection (1), the Department has the following powers:

(a) to investigate on the implementation of digital transformation across all public bodies, including the management of digital and cyber threats; and

(b) to direct, coordinate, and ensure coherence of ICT initiatives across all ministries, departments, and public agencies.

Division 3 Functions and powers of the Director

5 Functions of the Director

The Director has the following functions:

(a) to advise the Minister on any matters relating to digital transformation; and

(b) to oversee and coordinate the development and implementation of programs relating to internet governance, cybersecurity, and digital transformation; and

(c) to encourage innovation, local content development, and the responsible use of digital technologies; and

(d) to engage with civil society, industry stakeholders, and the public to promote digital literacy and awareness on digital transformation; and

(e) to coordinate the implementation of e-government initiatives to improve public service delivery and digital governance; and

(f) to oversee the implementation of the Digital Transformation Initiatives and the key ICT policies of the Government; and

(g) to ensure the development and maintenance of secure, accessible, and user-centric digital platforms for Government services; and

(h) to oversee, verify, and certify all ICT projects, systems, and procurements across government; and

(i) such other functions as may be imposed of the Director by this Act or any other Act.

6 Powers of the Director

(1) The Director has the power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions under this Act.

(2) Without limiting the generality of subsection (1), the Director has the following powers:

(a) to investigate and take enforcement action in relation to any breach or non-compliance by a public agency, private operator, or permit holder; and

(b) to issue or withhold Certificates of Compliance (CoC) for any ICT projects and suspend any project that commences without certification.

Division 4 Delegation of functions and powers of the Director

7 Delegation of functions and powers

(1) Subject to this section, the Director may delegate his or her functions and powers to a staff of the Department.

(2) The Director cannot delegate the power of delegation.

(3) A delegation made under subsection (1) is subject to instructions, guidelines or conditions imposed by the Director.

(4) A delegation under this section does not prevent the exercise of any powers by the Director.

(5) A delegation under this section may be revoked by the Director at any time.

Division 5 National Digital Transformation Steering Committee

8 Establishment of the National Digital Transformation Steering Committee

The National Digital Transformation Steering Committee is established.

9 Composition of the Committee

The Committee consists of the following persons:

(a) the Director General who is to be the Chairperson of the Committee; and

(b) the Director who is to be the Deputy Chairperson of the Committee; and

(c) the Director General of the Ministry of Finance and Economic Management; and

(d) the Director General of the Ministry of Foreign Affairs, International Cooperation and External Trade; and

(e) the Director General of the Ministry of Internal Affairs; and

(f) the Director General of the Ministry of Infrastructure and Public Utilities; and

(g) the Director General of the Ministry of Meteorology, Geological Hazards and Climate Change; and

(h) the Director General of the Ministry of Education and Training; and

(i) the Director General of the Ministry of Agriculture, Livestock, Forestry, Fisheries and Biosecurity; and

(j) the Director General of the Ministry of Land and Natural Resources; and

(k) the Director General of the Ministry of Tourism, Trade and Commerce and Ni-Vanuatu Business Development; and

(l) the Director General of the Ministry of Justice, Youth and Community Services; and

(m) the Director General of Fisheries, Ocean and Maritime Affairs; and

(n) the Regulator of Telecommunications, Radiocommunications and Broadcasting; and

(o) the Chief Executive Officer of the Digital Safety Authority; and

(p) a representative of the Reserve bank of Vanuatu to be nominated by the Governor General of the Reserve Bank of Vanuatu; and

(q) 2 representatives of the ICT sector nominated by the Director; and

(r) a representative of the Civil Society to be nominated by the President of the Vanuatu Association of Non-Government Organization.

10 Functions of the Committee

The Committee has the following functions:

(a) to develop and oversee the national Digital Transformation vision and overarching strategy, and ensure that it aligns with the national development goals such as the economic growth, service delivery, and social inclusion; and

(b) such other functions as may be imposed of the Committee by this Act or any other Act.

11 Powers of the Committee

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

(2) Without limiting the generality of subsection (1), the Committee has the following powers:

(a) to approve all Government or national ICT, Digital Transformation, Internet Governance, and Cyber Security strategies, policies, plans, and top initiatives before submission to the Council of Ministers; and

(b) to approve high-level oversight and direction plans for the national Cyber Security and ICT risk Management frameworks; and

(c) to approve and mandate common technical and architectural standards for government ICT infrastructure and digital services, thereby ensuring seamless integration and secure operations across the public sector; and

(d) to approve high-level national cyber security frameworks, policies, and strategies, and to ensure its effective implementation across the

nation, by coordinating efforts to safeguard critical information infrastructure.

12 Meetings of the Committee

(1) The Committee is to meet at least 2 times in a year in its ordinary meetings and may hold extraordinary meetings as are necessary for the proper performance of its functions under this Act.

(2) The Chairperson of the Committee is to preside at all meetings of the Committee and in his or her absence, the Deputy Chairperson is to preside at these meetings.

(3) The Department is the secretariat of the Committee.

(4) The quorum for a meeting of the Committee is 10 members of the Committee, present at the meeting.

(5) A member present at a meeting of the Committee has one vote and questions arising at a meeting are to be decided by a majority of votes.

(6) If the voting at a meeting is equal, the Chairperson or the Deputy Chairperson (if he or she is presiding over the meeting) has a casting vote.

(7) Subject to this Act, the Committee may determine and regulate its own procedures.

PART 3 ICT SERVICE PERMITS

13 Classes of ICT service permits

The following are the classes of ICT service permits that may be granted by the Director:

(a) an ICT companies permit; or

(b) a telecommunication provider permit; or

(c) a cloud provider permit; or

(d) a software vendor permit; or

(e) a hardware vendor permit; or

(f) an ICT consultancy permit; or

(g) an internal ICT department permit; or

(h) a virtual asset service provider permit; or

(i) an e-commerce and commercial multimedia streaming provider permit; or

(j) a cyber security operation center service permit; or

(k) an offshore digital service provider permit; or

(l) an artificial intelligence (AI) and AI-related data services permit; or

(m) a cybersecurity governance, risk and compliance services permit.

14 Application for an ICT service permit

(1) A person which intends to carry on business as an ICT service provider must apply to the Director for an ICT service permit.

(2) The Director may require an applicant, to provide additional information or documents that he or she considers necessary to decide on the application.

(3) If a request is made under subsection (2), the applicant must, within the time specified by the Director, provide the additional information and documents.

(4) The applicant must immediately inform the Director of the changes to the information provided to the Director under subsection (2).

(5) The Director may make any other inquiries in connection with the application as he or she considers necessary to be able to decide on the application.

(6) The Director is to consider the application and make a decision, within 14 working days of receiving the application.

15 Granting of an ICT service permit

(1) The Director may after receiving an application under section 14:

(a) grant an ICT service permit with or without conditions; or

(b) refuse to grant an ICT permit.

(2) The Director must, in making a decision under subsection (1), consider the following:

(a) the information supplied by the applicant is complete and not false or misleading; and

(b) the applicant has paid the prescribed fee; and

(c) any additional information and documents requested have been provided within the specified time; and

(d) there is no reason to believe that the applicant would not comply with the requirements of this Act and its Regulations; and

(e) the ICT standards.

(3) An ICT service permit is invalid if it is granted by the Director in contravention of the provisions of this Act.

16 ICT service permit conditions

(1) If the Director grants an ICT service permit under paragraph 15(1)(a) with conditions, the Director may, at any time:

(a) vary or revoke an ICT service permit condition; or

(b) impose further conditions on an ICT service permit.

(2) Before varying or revoking a condition, or imposing a further condition, the Director must give the ICT service permit holder notice, in writing, of the condition intended to be varied or revoked or of the further condition to be imposed.

(3) The ICT service permit holder must, within 14 working days after receiving the notice under subsection (2), give the Director reasons why the Director should not vary or revoke a condition or impose a further condition.

(4) The Director may impose, vary or revoke a condition or impose a further condition if:

(a) the ICT service permit holder fails to provide reasons to the Director reasons under subsection (3); or

(b) the Director is of the opinion that the ICT service permit holder has failed to show good cause why a condition should not be varied, revoked or further imposed.

(5) Despite subsection (3), if the Director is of the opinion that a condition imposed, varied or revoked should take effect immediately, the notice under subsection (2) must contain a statement to that effect, together with the reasons for that opinion.

17 Term of an ICT service permit

(1) An ICT service permit is valid for a period of 1 year.

(2) An ICT service permit remains in force until it is cancelled or surrendered under this Act.

(3) An ICT service permit holder must not assign or transfer an ICT service permit.

(4) A transfer of an ICT service permit has no effect.

18 Annual ICT service permit fee

An ICT service permit holder must pay the prescribed annual ICT service permit fee to the Director on or before each anniversary date of issuing of the ICT service permit.

19 Suspension of an ICT service permit

(1) If the Director is satisfied that:

(a) there is a breach of a condition of an ICT service permit; or

(b) there is a breach of a provision of this Act or its Regulations; or

(c) the ICT service permit holder is carrying out the ICT services in contravention of a provision of this Act or its Regulations,

the Director must, in writing, serve a notice of non-compliance on the ICT service permit holder as required under subsection (2).

(2) A notice of non-compliance must specify:

(a) the conditions of the ICT service permit or provision of the Act or its Regulation that was breached; and

(b) the penalty payable under the permit; and

(c) the period the penalty must be paid; and

(d) the period the breach is to be rectified.

(3) If the ICT service permit holder fails to rectify the breach of the ICT service permit or fails to pay the penalty within the period specified in the notice, the Director must:

(a) serve a notice of suspension to the ICT service permit holder; and

(b) allow the ICT service permit holder to provide reasons why the ICT service permit should not be suspended.

(4) If the Director is satisfied with the reasons provided under paragraph (3)(b), the Director may refuse to suspend the ICT service permit.

(5) If the Director is not satisfied with the reasons provided under paragraph (3)(b), the Director may suspend the ICT service permit.

(6) Despite subsection (1), if the Director is satisfied that there is a serious breach of the ICT service permit, the Director must suspend the ICT service permit.

(7) All operations must cease until the Director advises the ICT service permit holder that the suspension is lifted.

20 Cancellation of an ICT service permit

Subject to section 21, the Director may cancel an ICT service permit, if;

(a) the ICT service permit holder fails to comply with paragraph 19(3)(b); or

(b) the ICT service permit is suspended under subsection 19(6) and the serious breach of the ICT service permit has not been remedied to the satisfaction of the Director; or

(c) it appears to the Director that the ICT service permit holder:

(i) has been convicted of an offence under this Act; or

(ii) has breached any provisions of this Act or its Regulations.

21 ICT service permit holder to have opportunity to make representations before an ICT service permit is cancelled

(1) Prior to cancelling an ICT service permit under this Act, the Director must give the ICT service permit holder concerned a notice, in writing, specifying the grounds on which he or she intends to cancel the ICT service permit.

(2) The Director must inform the ICT service permit holder in the notice of his or her opportunity to submit his or her written statement of representations against the intended cancellation, within such time as may be determined by the Director.

PART 4 ENFORCEMENT OFFICERS

22 Appointment of enforcement officers

(1) The Director may appoint the following persons to be enforcement officers for the purposes of this Act:

(a) a senior officer in the Department; and

(b) a senior staff of the Digital Safety Authority; and

(c) senior police officer.

(2) The Director must issue an identity card to an enforcement officer which must contain a recent photograph of the enforcement officer.

23 Functions of an enforcement officer

The functions of an enforcement officer are to ensure that the provisions of this Act and its Regulations are complied with.

24 Powers of an enforcement officer

An enforcement officer has the power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions under this Act.

25 Inspection

(1) The enforcement officer may enter:

(a) any premises at any time with the consent of the occupier; or

(b) business premises during business hours at the premises; or

(c) premises when open to the public.

(2) When seeking the consent of an occupier for entering premises, an enforcement officer must:

(a) produce his or her identity card; and

(b) inform the occupier:

(i) of the purpose of the entry; and

(ii) that anything found and seized may be used as evidence in Court; and

(iii) that his or her consent may be refused.

(3) In carrying out an inspection, an enforcement officer must:

(a) avoid any damage or inconvenience; and

(b) not remain on the premises any longer than is reasonably necessary; and

(c) leave the premises so far as practicable in the same condition as it was found prior to the inspection being carried out.

26 Powers on entry

(1) An enforcement officer may do all or any of the following:

(a) inspect and take copies of any books, accounts and documents of the permit holder that relate to:

(i) a service provided by the permit holder;

(ii) the permit holder's other business, so far as it affects services provided by the permit holder;

(b) for a former permit holder- inspect and take copies of the former permit holder's books, accounts and documents that relate to the former permit holder's former provision of services;

(c) require information from the permit holder and directors of the permit holder about the services it provides;

(d) require information from the former permit holder about its former provision of services;

(e) search the premises and anything found at the premises, inspect and take photographs (including video recordings) that are related to the search only, or make sketches, of the premises or anything on the premises;

(f) inspect, and make copies of, or take extracts from, any document kept on the premises;

(g) seize anything on the premises the enforcement officer believes on reasonable grounds is necessary to be seized in order to prevent its concealment, loss or destruction;

(h) take into the premises any equipment or material the enforcement officer reasonably needs for exercising a power under this Part;

(i) require the occupier, or a person on the premises, to give the enforcement officer reasonable help to exercise a power under this Part.

(2) The permit holder must cooperate fully with the enforcement officer by:

(a) giving the enforcement officer all the information, and making available the documents it requires; and

(b) if necessary, give the enforcement officer appropriate workspace and reasonable access to office services, during the inspection.

27 Seizure of ICT materials

(1) If an enforcement officer has reasonable grounds to believe an offence against this Act or its Regulations is being or has been committed, he or she must seize any ICT materials relevant to the commission of the offence.

(2) The seized ICT materials must be stored in an area approved by the Director until they are destroyed or disposed of as the Director in writing directs.

28 Receipt for things seized

(1) An enforcement officer must confirm in writing to the permit holder, the receipt of the thing seized from the permit holder, immediately after a thing is seized by the enforcement officer.

(2) If, for any reason, it is not practicable to comply with subsection (1), the enforcement officer must leave the confirmation in writing and secured at a place to be visible to the occupier.

29 Return of things seized

(1) If an enforcement officer seizes a thing, the enforcement officer must take reasonable steps to return it to the permit holder from whom it was seized if the reason for its seizure no longer exists.

(2) If the item has not been returned within 14 days after it is seized, the enforcement officer must take reasonable steps to return it unless:

(a) proceedings have commenced and those proceedings have not been completed; or

(b) the Court makes an order under subsection (3), extending the period of 14 days.

(3) An enforcement officer may apply to the Court before the expiration of the 14 days period or within a period extended by the Court for an extension of that period.

(4) The Court may order an extension if satisfied that the retention of the thing is necessary for the purposes of an investigation into whether an offence has been committed or to enable evidence of an offence to be obtained for the purposes of a prosecution.

(5) The enforcement officer must notify the person of any application made under subsection (3).

30 Search Warrants

(1) The Director or an enforcement officer may apply to the Court for a search warrant:

(a) to enter:

(i) premises belonging to, or in the possession or control of, an ICT service permit holder or an employee of an ICT Service Permit holder; or

(ii) any other premises that the Director or enforcement officer has reasonable grounds for believing that it contains documents relating to the provision of services by the ICT service permit holder or relevant to an investigation; and

(b) to search the premises and take copies of, or remove, any document, equipment or material from the premises.

(2) The Court may issue a search warrant if it is satisfied on reasonable grounds that:

(a) there is a particular thing ('the evidence') at the premises connected with an offence against this Act; or

(b) failure to obtain the search warrant would prejudice an investigation; or

(c) there is a reasonable likelihood that the documents sought are on the premises and could be altered, destroyed or removed.

(3) If an enforcement officer removes a document from the premises under a search warrant, the officer must leave a copy of the document at the premises.

PART 5 OFFENCES AND PENALTY NOTICE

31 Offences

(1) A person who carries out an ICT activity without a valid permit, commits an offence and is punishable on conviction:

(a) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(2) A person who contravenes a provision of this Act commits an offence, punishable on conviction:

(a) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(3) A person who recklessly or negligently makes any representation under this Act that the person knows to be false or misleading commits an offence and is liable on conviction:

(a) for an individual- to a fine not exceeding VT3,000,000 or imprisonment for a term not exceeding 3 years, or to both; and

(b) for a body corporate- to a fine not exceeding VT20,000,000.

(4) A person who obstructs the Director or any person authorised by the Director in performing any of his or her duties under this Act, commits an offence and is liable on conviction to a fine not exceeding VT3,000,000 or imprisonment for a term not exceeding 3 years or to both.

(5) A person who:

(a) gives false or misleading information to an enforcement officer that the person knows to be false or misleading; or

(b) produces a document to an enforcement that the person knows to be false or misleading,

commits an offence and is liable on conviction to a fine not exceeding VT 3,000,000 or to imprisonment for a term not exceeding 3 years, or to both.

(6) If a person without reasonable excuse obstructs or hinders an enforcement officer in exercising any power under this Act, the person commits an offence and is liable on conviction to a fine not exceeding VT 3,000,000, or to imprisonment for a term not exceeding 3 years, or to both.

(7) If a person impersonates an enforcement officer, the person commits an offence and is liable on conviction to a fine not exceeding VT 3,000,000, or to imprisonment for a term not exceeding 3 years, or to both.

(8) A person who intentionally obstructs a person in the execution of a search warrant issued under this Act commits an offence, punishable on conviction, by a fine not exceeding VT3,000,000.

32 Penalty notice

(1) The Director may serve a penalty notice on a person if it appears to the Director that the person has committed an offence under any provision of this Act.

(2) A penalty notice is a notice to the effect that if the person served does not wish to have the matter determined by a Court, the person may, within a time and to a person specified in the notice, pay the amount of penalty stated in the penalty notice.

(3) A penalty notice may be served personally, by post or email.

(4) If the amount of penalty prescribed for the purposes of this section for an alleged offence is paid under this section, no person is liable to any further proceedings for the alleged offence.

(5) Payment under this section is not to be regarded as an admission of liability for the purpose of, nor in any way affect or prejudice, any civil proceeding arising out of the same occurrence.

(6) The Regulations may prescribe the amount of penalty payable for the offence if dealt with under this section.

(7) The amount of a penalty prescribed under this section for an offence must not exceed the maximum amount of penalty provided for in this Act.

PART 6 MISCELLANEOUS PROVISIONS

33 Cyber security incidents

(1) The Director must provide a written report to the Minister and the National Security Council, on any significant cyber security incident affecting government services, critical infrastructure or supply chain services.

(2) The report under subsection (1) must be made not later than 72 hours after the cyber security incident has been identified.

34 Annual reports

The Director must within 3 months after the end of each financial year provide a report to the Minister relating to the operations of the Department for the preceding year.

35 Protection from liability

(1) A civil or criminal proceeding must not be brought against the Director, any employee of the Department or any enforcement officer for anything done or omitted to be done in good faith by him or her in carrying out his or her functions or in exercising his or her powers under this Act.

(2) Subsection (1) does not apply if the Director, any employee of the Department or any enforcement officer acted in bad faith in performing his or her functions or exercising his or her powers under this Act.

36 Rules

(1) The Director may make rules, not inconsistent with this Act and any Regulations made under section 37, determining matters that are required or permitted to be determined by the Director.

(2) A rule made under this section may apply generally to all permit holder and government users.

37 Regulations

The Minister may make Regulations prescribing all matters:

(a) required or permitted by this Act to be prescribed; or

(b) that are necessary or convenient to be prescribed for the carrying out or giving effect to the provisions of this Act.

38 Commencement

This Act commences on the day on which it is published in the Gazette.