No. 41 of 2022.

***Digital Government Act* 2022.**

Certified on : 19 JUL 2022

No. 41 of 2022.

ARRANGEMENT OF SECTIONS.

***Digital Government Act* 2022.**

PART I. - PRELIMINARY.

PART V. - ELECTRONIC DATA.

PART VI. - ENFORCEMENT.

PART VII. - OFFENCES.

PART VIII. - MISCELLANEOUS.

No. 41 of 2022.

AN ACT

entitled

***Digital Government Act* 2022,**

Being an Act to -

(*a*) provide for digital government through the use of information and communication technologies; and

(*b*) enable the streamlining, planning, coordination, development and implementation across the whole of government of digital services, digital infrastructure, digital skills and all other aspects of digital government,

and for related purposes,

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

PART I. - PRELIMINARY.

1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS.

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 freedom of employment conferred by Section 48; and

(*d*) the right to privacy conferred by Section 49; and

(*e*) the right to freedom of information conferred by Section 51; and

(*f*) the right to protection from unjust deprivation of property conferred by Section 53,

of the ***Constitution***, is a law that is made pursuant to Section 38 of the ***Constitution*** taking account of the National Goals and Directive Principles and Basic Social Obligations, for the purpose ofgiving effect to the public interest in public order, public safety and public welfare.

2. INTERPRETATION.

In this Act, unless the contrary intention appears -

"application" means a distinct set of machine instructions that are interpretable and executableby a computing device and designed to fulfil a particular purpose;

"application programming interface" or "API" means any software application or hardware technology or any combination of the two that is designed to facilitate integration or interoperability of two or more systems;

"Central Electronic Data Repository" means the Central Electronic Data Repository established under Section 28 as the official storage server to backup electronic data of public bodies and provide safety against potential unforeseen events that may cause data loss to public bodies;

"Classified Data" means an electronic data classified under Section 45 as top-secret data, confidential data and open data;

"Cloud Infrastructure" means the numerous data centres managed by Cloud Services Providers (third party vendors) located throughout the world that have installed hardware necessary for providing cloud-based solutions like servers, networks, storage, development tools and applications (apps) accessible virtually via the Internet;

"critical digital infrastructure" has the meaning given by Section 21;

"data traffic prioritisation network algorithm" means a computer program or computer instruction used to solve and manage data flows or efficient routing of data traffic;

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

"digital government" includes the use of ICT by government to deliver digital services and develop digital infrastructure and digital skills;

"Digital Government Plan" means the Digital Government Plan developed under Section 10;

"digital infrastructure" is any device or mechanism used to or capable of delivering data and digital services, and may be physical or virtual, or hardware or software and includes, but is not limited to the following:

(*a*) the Central Electronic Data Repository; and
(*b*) the National Electronic Data Bank, data registers; and
(*c*) ICT platforms; and
(*d*) cloud infrastructure; and
(*e*) the Government Cloud Infrastructure; and
(*f*) the Government Private Network and other networks; and
(*g*) systems; and
(*h*) software applications; and
(*i*) APIs and integration; and
(*j*) endpoint devices; and
(*k*) internet exchange points; and
(*l*) servers, routers and modems enabling system connectivity of virtual private networks and wireless by-pass links; and
(*m*) telecommunication infrastructures such as broadband, satellite connectivity, radio links, optic fibre, dark fibre, copper cables and all other related systems;

"digital services" means internet enabled services that are delivered and accessed using digital infrastructure;

"digital transformation officer" means the person who has oversight of, and is responsible for ICT matters in a public body, and he is deemed to be a delegate of the head of a public body with respect to ICT matters;

"electronic data" means data entered into an electronic device to be processed, generated, sent, received, stored or shared using a system or device for the purposes of enabling the delivery of digital services and includes, but is not limited to, any representation of facts, concepts and information in the form of text, image, audio, video, multimedia file and machine-readable code or instructions;

"Electronic Data Register" means the Electronic Data Register established under Section 51;

"endpoint device" means an internet capable device that communicates across a network, such as laptops, telephones and personal computers;

"government domain" means the domain ending in gov.pg;

"Government Leased Cloud Infrastructure" means the cloud infrastructure owned by a cloud service vendor and used by the Department under a commercial arrangement for government cloud services established under Section 25;

"Government Private Cloud Infrastructure" means the cloud infrastructure owned by the Government under Section 26;

"Government Private Network" means the Government Private Network referred to in Section 22;

"guideline" means a guideline made by the Department under Section 64;

"ICT" means information and communications technology;

"ICT Audit Committee" means the Public Service ICT Audit Committee established under Section 16;

"ICT Project Design" means an ICT Infrastructure plan of a public body to deliver digital Government;

"ICT Steering Committee" means the Public Service ICT Steering Committee established under Section 11;

"National Cyber Security Centre" or "NCSC" means the National Cyber Security Centre referred to in Section 18;

"National e-Government Online Portal" means the National e-Government Online Portal established under Section 35;

"National Electronic Data Bank" means the National Electronic Data Bank referred to in Section 27;

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

"Officer" means an officer or employee of the Department;

"open data" means any government electronic data that any person can access, use and share, and is deemed public data under Section 36;

"public body" means -

(*a*) any agency which is part of the state services established under Part VII and Part VIIA of the ***Constitution***; and

(*b*) any statutory body as defined under the ***Public Finances (Management) Act*** **1995**; and

(*c*) a Provincial Government or Local-level Government established under the ***Organic Law on Provincial Governments and Local-level Governments*** but does not include a majority owned state enterprise;

"***Public Services (Management) Act***" means the ***Public Services (Management) Act*** **1995**;

"Secretary" means the Secretary for the Department of Information and Communication Technology;

"shared service" means the consolidation of digital infrastructure of public bodies into a stand-alone digital infrastructure as an internal service for public bodies to use to provide digital services;

"system" means a digital infrastructure set-up consisting of hardware, software or a group of interconnected physical or virtual devices, one or more of which under a program, performs automatic processing, generating, sending, receiving or storing of electronic data to produce a specific output;

"systems integration" means connecting one or more systems so that electronic data from one system can be used by another to enable information exchange to deliver digital services;

"systems interoperability" means the ability of different systems to communicate and exchange electronic data in real-time and use the data that has been exchanged;

"Top-Secret Data" has the meaning under Section 45(1).

3. APPLICATION.

(1) This Act binds the State.

(2) This Act applies to all public bodies to the extent that it does not prevent the proper discharge of ICT regulatory functions and powers established under ***National Information and Communications Technology Act*** **2009**.

(3) This Act is not intended to apply to state-owned enterprises.

4. APPLICATION OF ELECTRONIC EVIDENCE RULE.

(1) Subject to Subsections (2) and (3), rules of electronic evidence set out in the ***Evidence Act*** (Chapter 48) applies to all electronic data under this Act.

(2) In any legal proceeding, data stored in the Central Electronic Data Repository is not admissible as evidence of any fact, unless by an order of the National or Supreme Court.

(3) Top-Secret Data is not admissible evidence of any fact.

PART II. - ADMINISTRATION.

Division 1. - General administration.

5. ADMINISTRATION OF THE ACT.

Unless otherwise stipulated in this Act, the Departmental Head of the Department is to administer this Act.

6. FUNCTIONS OF THE DEPARTMENT.

(1) The functions of the Department, administered by the Departmental Head, are -

(*a*) to develop and update ICT policies; and
(*b*) to co-ordinate general operational matters relating to ICT for public bodies; and
(*c*) to co-ordinate the construction and delivery of whole of government digital infrastructure and digital services; and
(*d*) to support operations with agencies responsible for national intelligence and national security to ensure cyber security and safety are maintained across whole of government; and
(*e*) to establish and maintain a whole of government register of systems, digital infrastructure and digital services; and
(*f*) to develop plans as necessary for the purposes of delivering digital services; and
(*g*) to ensure public bodies comply with this Act; and
(*h*) to institute proceedings for offences against this Act; and
(*i*) to perform such other functions conferred on the Department by this Act, an instrument or any other law.

(2) The functions of the Department under Subsection (1) are in addition to its functions conferred by the ***Public Services (Management) Act* 1995**.

7. POWERS OF THE DEPARTMENT.

The Department has, in addition to the powers conferred on it by this Act or any other law, powers to do all things necessary or convenient to be done or in connection with the performance of its functions.

8. DELEGATION.

(1) The Departmental Head may delegate to an officer of the Department, any of his powers or functions under this Act except for the power of delegation.

(2) A delegation under Subsection (1) shall be in writing.

9. DIGITAL TRANSFORMATION OFFICERS.

(1) A public body shall designate a digital transformation officer for the purposes of this Act.

(2) A digital transformation officer is -

(*a*) to co-ordinate with the Department on ICT and digital transformation matters; and
(*b*) to facilitate integration and interoperability of the systems of the public body; and
(*c*) to facilitate delivery of digital services by the public body; and
(*d*) to manage the electronic data in the public body; and

(*e*) to provide ICT reports and feedback on a quarterly basis to the Department or as requested by the Secretary.

(3) Where a public body does not have a digital transformation officer, the head of the public body shall nominate an officer to perform the functions of a digital transformation officer until such time a digital transformation officer has been designated.

(4) The Department shall, in collaboration with other relevant agencies, take all steps necessary to develop and ensure digital skills and digital government capacity building programs are available to digital transformation officers.

10. DIGITAL GOVERNMENT PLAN.

(1) The Departmental Head is to formulate a Digital Government Plan to deliver digital services.

(2) The ICT Steering Committee shall review the proposed Digital Government Plan before the Department finalises the Plan.

(3) The Departmental Head is to circulate the approved Digital Government Plan to all public bodies and all public bodies must comply with the Plan.

(4) The Departmental Head shall review and update the Digital Government Plan every five years or as advised by the Minister in accordance with a NEC Decision.

(5) A public body shall, in accordance with the relevant guidelines, conduct an annual self-assessment of its implementation of the Digital Government Plan and submit the assessment to the Departmental Head on or before the end of the year to which the assessment relates.

(6) A person who fails to comply with Subsection (5) commits an offence against this Act.

Division 2. - Committees.

11. PUBLIC SERVICE ICT STEERING COMMITTEE.

(1) The Public Service ICT Steering Committee is hereby established.

(2) The ICT Steering Committee shall consist of the following persons:

(*a*) the Departmental Head of the Department or his nominee; and

(*b*) the digital transformation officer of the Department responsible for finance matters or his nominee; and

(*c*) the digital transformation officer of the Department responsible for treasury matters or his nominee; and

(*d*) the digital transformation officer of the Department responsible for national planning and monitoring matters or his nominee; and

(*e*) the digital transformation officer of the Department responsible for justice matters or his nominee; and

(*f*) the digital transformation officer of the Department responsible for personnel management matters or his nominee; and

(*g*) the digital transformation officer of the Department responsible for provincial and local government affairs or his nominee; and

(*h*) a representative from the public body whose digital transformation matter is to be considered by the Committee or his nominee; and

(*i*) any other person in the ICT industry, the Secretary may invite from time to time.

(3) The Departmental Head is the Chairman of the Committee, or in his absence, his nominee from the Department.

12. FUNCTIONS OF THE ICT STEERING COMMITTEE.

The functions of the ICT Steering Committee are -

(*a*) to facilitate the formulation, implementation and review of the Digital Government Strategic Plan across all public bodies; and

(*b*) to serve as a government forum for awareness on ICT policies, laws, programs and projects in relation to public bodies; and

(*c*) to assist the Departmental Head to identify and evaluate public bodies' digital infrastructure and digital government programs and projects; and

(*d*) to evaluate ICT Project Designs of public bodies and make recommendations to the Departmental Head to approve or reject a design; and

(*e*) to assist the Departmental Head to identify ICT policy gaps and make recommendations to address them; and

(*f*) to assist the Department give effect to ICT policy directions of the government; and

(*g*) to perform any other technical and advisory function as is necessary in connection with this Act.

13. MEETINGS OF THE ICT STEERING COMMITTEE.

(1) At a meeting of the ICT Steering Committee, five members, one of whom shall be the Departmental Head or his nominee, constitutes a quorum.

(2) The ICT Steering Committee shall meet as often as necessary for the implementation of this Act and at such times and places as the Committee determines, or as the Chairman or his nominee directs, but in any event shall meet at least once in every quarter.

(3) The meetings of the ICT Steering Committee may be conducted either physically or virtually as determined by the Committee, or as directed by the Chairman or his nominee.

(4) Subject to Subsection (7), the Chairman or his nominee shall give to every member at least 3 working days written notice of the meeting.

(5) The invitation may be sent by authenticated electronic means or a written notice, or both and must include the meeting agenda.

(6) A member who has a conflict of interest in any agenda to be discussed must declare and abstain from voting or participating in the agenda discussion.

(7) The Chairman may call an emergency meeting at anytime and not less than three members shall constitute the quorum.

(8) The ICT Steering Committee shall cause minutes of its meetings and resolutions to be recorded and kept.

(9) The Chairman or his nominee must circulate to all members approved meeting minutes and resolutions not later than 30 days after the day the meeting was held.

14. APPROVAL FOR ICT ASPECTS OF PROJECT DESIGNS.

(1) A public body shall not adopt or purchase and use an ICT Project Design unless a request is made in writing and approved by the Departmental Head.

(2) A public body that intends to adopt or purchase and use an ICT Project Design shall obtain written approval from the Departmental Head.

(3) On receipt of an approval request under Subsection (1), the Departmental Head must respond in writing within 30 days from the date of receipt or within such period extended by the Departmental Head in writing.

(4) The Departmental Head shall approve or reject an ICT Project Design of a public body -
- (*a*) if the sum of the projected cost of the project design in a year is K5,000,000.00 or more, based on the recommendation of the ICT Steering Committee; or
- (*b*) if the sum of the projected cost of the project design is less than K500,000.00, by the Departmental Head.

(5) If the Department approves the ICT Project Design, the Departmental Head shall issue a Certificate of Compliance to the public body making the request within 10 days from the date of the decision.

(6) If the Departmental Head rejects the ICT Project Design, he shall issue a written notice of his rejection to the public body within 10 working days of the decision.

(7) If the decision is not communicated to the public body making the request within the required time under Subsection (5), it would be deemed that the request is rejected.

(8) For avoidance of doubt, this section applies to approval of ICT Project Design before procurement process under any law may take effect.

15. CERTIFICATE OF COMPLIANCE FOR PUBLIC INVESTMENT PROGRAM AND STATE GUARANTEED ICT PROJECT DESIGN.

(1) This section applies to an ICT Project Design proposed by a public body where it requires -
- (*a*) development budget funding from the government; or
- (*b*) State guaranteed funding.

(2) An ICT Project Design to which this section applies must comply with the Digital Government Plan or relevant ICT sector plan, the ICT policies of the government and this Act.

(3) A public body must obtain a Certificate of Compliance before submitting -
- (*a*) its work plan and cash flow plan to the department responsible for development budget matters; or
- (*b*) its proposal to the department responsible for issuing state guarantee on project funding.

(4) An approved ICT Project Design is deemed to form part of the National Planning Framework under the ***Papua New Guinea Planning and Monitoring Responsibility Act* 2016** for funding consideration.

(5) If a Certificate of Compliance is not issued for an ICT Project Design of a public body, it shall not be considered for development budget funding or State guaranteed funding.

(6) The head of a public body who fails to obtain a Certificate of Compliance before seeking funding under Subsection (1), commits an offence.

16. PUBLIC SERVICE ICT AUDIT COMMITTEE.

(1) The Public Service ICT Audit Committee is hereby established.

(2) The ICT Audit Committee shall consist of -

(*a*) the Deputy Departmental Head in charge of digital matters of the Department or his nominee; and

(*b*) a representative of the Auditor-General's Office nominated by the Auditor-General; and

(*c*) a Lawyer from the State Solicitor's Office nominated by the State Solicitor; and

(*d*) a representative from the Department responsible for public finance matters nominated by the Departmental Head of that Department; and

(*e*) a representative from the Department responsible for personnel matters nominated by the Departmental Head of that Department; and

(*f*) a representative from the National Information and Communication Technology Authority nominated by its Chief Executive Officer; and

(*g*) a representative of the Papua New Guinea Information Systems Audit and Control Association; and

(*h*) a person nominated by the Departmental Head.

(3) The Departmental Head shall determine the Chairperson of the Committee.

(4) The ICT Audit Committee shall meet if the Departmental Head considers it necessary that the Committee assesses and evaluates a public body's use of a system against regulations, standards or specifications under this Act.

(5) The ICT Audit Committee is to regulate the conduct of proceedings at its meetings as it thinks fit.

17. FUNCTIONS OF THE ICT AUDIT COMMITTEE.

(1) The ICT Audit Committee shall -

(*a*) perform ICT audits on the systems used by public bodies at least once in a year; and

(*b*) perform other functions as are set out in the Committee's terms of reference as prescribed by the Departmental Head.

(2) In conducting an ICT audit, the Committee shall evaluate the systems used by a public body by -

(*a*) reviewing all or any of the following:

(i) the ICT organisational structure of the public body; or

(ii) the public body's internal ICT policies and procedures; or

(iii) the public body's compliance with this Act and the Regulations, standards and specifications; or

(iv) ICT documentation and ICT projects of the public body; or

(v) risk associates with the use of a system; and

(*b*) interviewing the appropriate ICT personnel of the public body; and

(*c*) conducting such other audit activities as directed by the Departmental Head; and

(*d*) undertaking audits of -

(i) the systems of public bodies and other private systems offering services to public bodies; and

(ii) the digital infrastructure of public bodies.

(3) The Committee shall report its findings to the Departmental Head.

(4) The Committee, in addition to its findings, may recommend to the Departmental Head to engaged an independent specialised ICT auditor for further technical audit on a system used by a public body.

Division 3. - Centres.

18. NATIONAL CYBER SECURITY CENTRE.

(1) A National Cyber Security Centre is hereby established.

(2) The NCSC shall be jointly operated by -

(*a*) the Department; and
(*b*) the Department responsible for defence matters; and
(*c*) the Department responsible for police matters; and
(*d*) the Department responsible for justice matters; and
(*e*) the National Intelligence Office; and
(*f*) the Department responsible for Prime Minister and NEC matters.

(3) Any asset, equipment, system or apparatus used by the NCSC is, by force of this Section, transferred to the National Government.

(4) The Department shall continue to provide administrative oversight of the NCSC.

19. FUNCTIONS OF NATIONAL CYBER SECURITY CENTRE.

(1) The National Cyber Security Centre shall coordinate all efforts of national cyber security by performing the following functions:

(*a*) conduct defensive cyber security operations; and
(*b*) promote a secured digital government environment; and
(*c*) ensure government digital infrastructure contains appropriate security control technologies; and
(*d*) promote cyber resilience to ensure services that are essential for everyday life remain effective and operational during cyber threats and attacks; and
(*e*) investigate any breaches of cyber security and escalate security incidents to appropriate authorities (if necessary), for their intervention; and
(*f*) monitor and hunt cyber threats across networks and end points, and ensure that threats attacking data and assets are contained and eliminated; and
(*g*) provide the persons to whom the NCSC provides services with remote incident response and handling support; and
(*h*) conduct audits on cyber security tracking and monitoring systems and end point devices used by public bodies; and
(*i*) establish procedures for the persons to whom the NCSC provides services and other member organisations of the Papua New Guinea Computer Emergency Response Team to report cyber-attacks or suspected cyber incidents; and
(*j*) provide regular reports to the persons to whom the NCSC provides services; and
(*k*) provide technical support to the Papua New Guinea Computer EmergencyResponse Team; and
(*l*) recommend to the Departmental Head the prosecution of relevant offences; and
(*m*) perform other activities as directed in writing by the Departmental Head.

(2) In addition to its functions referred to in Subsection (1), the NCSC may -

(*a*) provide technical censorship support services to a public body responsible for censorship matters; and
(*b*) by agreement with another person, provide cyber security services to that other person.

(3) The Departmental Head may, acting on the recommendation of the NEC, outsource all or any of the functions of the NCSC.

PART III. - DIGITAL INFRASTRUCTURE.

20. DIGITAL INFRASTRUCTURE.

The Department shall co-ordinate the delivery of digital infrastructure and critical digital infrastructure under this Part.

21. CRITICAL DIGITAL INFRASTRUCTURE.

(1) Critical digital infrastructure is digital infrastructure that is -

(*a*) owned by the State; and

(*b*) essential for the functioning of the government, the economy and the society as a whole.

(2) Critical digital infrastructure includes, but is not limited to the following:

(*a*) National Electronic Data Bank; and

(*b*) Central Electronic Data Repository; and

(*c*) Subject to Subsection (1), Government Private Network; and

(*d*) Secured Data Exchange platform; and

(*e*) National Cyber Security Centre.

(3) Subject to Subsections (1), the Minister acting on advice of the NEC may, in writing, designate other digital infrastructure as critical digital infrastructure.

(4) Critical digital infrastructure must not be installed, changed, reconstructed, replaced, repurposed or removed by any person unless the Minister directs in writing in accordance with a NEC decision.

(5) For avoidance of doubt, a software-based application or other digital infrastructure shall not be a critical digital infrastructure, if the application or other digital infrastructure is owned by a person, other than the State, even if it is available to a public body under a software as a service arrangement or any other agreement.

22. GOVERNMENT PRIVATE NETWORK.

(1) A Government Private Network is hereby established.

(2) The Government Private Network by the Department and is to consist of -

(*a*) the Central Electronic Data Repository; and

(*b*) any physical, virtual or cloud networks connectivity operated by the Department or a public body approved by the Department; and

(*c*) various types of shared services, including digital infrastructure, internet and software as services to enhance network connectivity and electronic data sharing amongst public bodies.

(3) For the avoidance of doubt, networks in Subsection (2)(*b*), does not preclude any portions or parts of the network infrastructure utilised by a public body that is owned by a commercial operator to be subject to Regulations under the ***National Information and Communications Technology Act* 2009**.

(4) All public bodies must use the Government Private Network or an alternative network approved under Section 23.

(5) The Government Private Network shall be managed by the Department or a public body approved by the Department in accordance with this Act.

23. ALTERNATIVE NETWORKS TO THE GOVERNMENT PRIVATE NETWORK.

(1) A public body must not use an alternate network to the Government Private Network unless approved by the Departmental Head.

(2) The head of a public body, that intends to use an alternate network to the Government Private Network, must make a written request to the Departmental Head for approval.

(3) A request under Subsection (2) is to be referred to the Departmental Head within 5 days from the date the request is received to consider and provide recommendations to the Departmental Head.

(4) Based on the recommendations of the ICT Steering Committee, the Departmental Head may reject or approve a request.

(5) The Departmental Head shall provide written notice to the public body of the decision under Subsection (3) within 5 days of the decision being made.

(6) If the decision is not communicated to the requesting public body within the required time under Subsection (5), it would be deemed that the request is rejected.

24. DATA TRAFFIC PRIORITISATION.

(1) Where the Government Private Network is not available to a public body, the Department may, in consultation with a network operator providing network services to the public body, deploy and operate data traffic prioritisation network technology on the operator's network.

(2) The purpose of operating data traffic prioritisation network technology on an ICT network is to -

(*a*) enable government data traffic passing through the ICT network to deliver quality of service; and

(*b*) improve the quality of service provided to the public body by enabling prioritisation of data traffic during periods of network congestion and in areas where the network infrastructure suppresses delivery of data; and

(*c*) improve the quality of service to the public body by shaping or constructing efficient routing or data flows in the ICT network for digital service delivery; and

(*d*) improve other quality of services with respect to data flows within the ICT network for the public body.

25. GOVERNMENT LEASED CLOUD INFRASTRUCTURE.

(1) The Department shall establish a Government Leased Cloud Infrastructure for connectivity of virtual private networks and digital services for all public bodies.

(2) The Departmental Head shall source the Government Leased Cloud Infrastructure from the register in Subsection (10).

(3) Within one year of the date of establishment of the Government Leased Cloud Infrastructure, all virtual private networks and digital services of public bodies that use a cloud infrastructure outside the Government Leased Cloud Infrastructure must migrate and operate within the Government Leased Cloud Infrastructure.

(4) If a public body intends to continue its operations outside the Government Leased Cloud Infrastructure, that public body must within 90 days from the date of establishment in Subsection (3), apply in writing for the Departmental Head's approval.

(5) The Departmental Head shall approve an application made by a public body in Subsection (4), if he is satisfied that -

(*a*) the cloud infrastructure used by the public body makes it practically impossible for the public body to migrate its virtual private network into the Government Leased Cloud; and

(*b*) the public body has specific requirements that the Government Leased Cloud Infrastructure is not able to provide.

(6) The Departmental Head shall give a written notice to the public body of his decision within 14 days from the date of receipt of the request.

(7) If the decision is not communicated to the public body requesting for approval within the required time under Subsection (6), it would be deemed that the request is approved.

(8) A person who, whether under a contract or otherwise, without approval of the Departmental Head under Subsection (6), operates or facilitates operations of a public body's virtual private network outside of the Government Leased Cloud Infrastructure, is guilty of an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K50,000.00 or imprisonment for a period not exceeding five years, or both; and

(*b*) In the case of an offence by a body corporate, a fine not exceeding K1,000,000.00.

(9) The Department must establish a register of Cloud Infrastructure vendors approved by the NEC and must keep the register up to date.

(10) The Government Leased Cloud Infrastructure ceases to operate, on the date Government Private Cloud Infrastructure is published in the National Gazette to be effective under Section 26(7).

26. GOVERNMENT PRIVATE CLOUD INFRASTRUCTURE.

(1) The Department may build a Government Private Cloud Infrastructure as part of the Government Private Network for delivery of digital services.

(2) If the Government Private Cloud Infrastructure is built, the Departmental Head shall ensure it is designed to meet prevailing international standards for security and system integrity assurance.

(3) Subject to Subsection (5), the Government Private Cloud Infrastructure operational centre is to be located in Papua New Guinea.

(4) Subject to Subsection (5), the electronic data of public bodies stored in the Government Leased Cloud Infrastructure, sanctioned by the Department under Section 25, must be migrated, stored and secured in the Government Private Cloud Infrastructure within -

(*a*) one year after the date the Government Private Cloud Infrastructure is commissioned by the Secretary as fully functional; or

(*b*) such longer period after that date as is determined by the Departmental Head.

(5) After the establishment of the Government Private Cloud Infrastructure, a public body may continue to use and store its electronic data on a cloud infrastructure outside of Papua New Guinea if -

(*a*) it will contribute to the efficient functioning of the public body; and
(*b*) the storage outside of Papua New Guinea satisfies all standards and specifications; and
(*c*) the Departmental Head acting on the advice of the ICT Steering Committee has given its written approval to the public body for storage outside of Papua New Guinea; and
(*d*) the public body undertakes to comply with any terms and conditions issued by the Departmental Head.

(6) A head of a public body who fails to comply with this section, commits an offence.

(7) This section takes effect, on the date the Government Private Cloud Infrastructure is commissioned by the Minister and is published in the National Gazette.

27. NATIONAL ELECTRONIC DATA BANK.

(1) The Department shall as soon as practicable, own a building known as the National Electronic Data Bank.

(2) The National Electronic Data Bank shall hold -

(*a*) the Central Electronic Data Repository; and
(*b*) the National Cyber Security Centre; and
(*c*) the Government Private Cloud Infrastructure if established; and
(*d*) any other data server of a public body in the National Electronic Data Bank; and
(*e*) all associated core infrastructure pertaining to Paragraphs (*a*) and (*b*).

(3) The National Electronic Data Bank shall have high security systems of international standards acceptable to the Department.

(4) The design of the National Electronic Data Bank and the final digital security architectural design shall be as approved by the Department.

(5) The design of the National Electronic Data Bank is classified as top-secret data under Section 45(1), and shall not be accessible by any person, except in accordance with this Act.

(6) The Department is to provide general oversight of the capital financing and construction of the National Electronic Data Bank.

(7) A person shall not conduct other business in the National Electronic Data Bank, unless otherwise approved by the Departmental Head in writing in accordance with this Act.

28. CENTRAL ELECTRONIC DATA REPOSITORY.

(1) The Department shall establish and manage the government's Central Electronic Data Repository.

(2) The Central Electronic Data Repository shall be the official storage server to backup electronic data of public bodies and provide safety against potential unforeseen events that may cause data loss to public bodies.

(3) The Central Electronic Data Repository shall consist of -

(*a*) a physical electronic data repository; and
(*b*) other redundancy data repositories established under Section 30,

that are synchronised and operating as one data storage sever for compulsory backup or redundant data storage for all public bodies.

(4) The Central Electronic Data Repository must contain -
(*a*) an active operational software and hardware server; and
(*b*) a storage software and hardware server; and
(*c*) a system processing software and hardware server.

(5) Subject to Subsection (6), a public body that stores its data by electronic means, shall as regularly as practicable, also have its electronic data backed up, in the Central Electronic Data Repository, as its redundancy, within one year on the date the Central Electronic Data Repository is established and published by the Minister in the National Gazette.

(6) If -
(*a*) a public body uses a system of international standards and those standards preclude the public body from backing up its data in the Central Electronic Data Repository; or
(*b*) for some other practical reason, the public body is precluded from backing up its data in the Central Electronic Data Repository,
the public body shall take all reasonable steps to have its data backed up in the Central Electronic Data Repository within three years from the date of publication in Subsection (5).

(7) The head of a public body who, fails to comply with this Subsection (5) and (6) commits an offence.

29. ACCESS TO CENTRAL ELECTRONIC DATA REPOSITORY.

(1) For the purpose of this section, access to the Central Electronic Data Repository means access to different sections of the physical and virtual database servers consisting of -
(*a*) physical access to the National Electronic Data Bank; and
(*b*) physical access to the holding vault of the main Central Electronic Data Repository; and
(*c*) physical and virtual access to the active operating system of the Central Electronic Data Repository.

(2) Except for open data, a person shall not obtain any electronic data stored in the Central Electronic Data Repository, unless -
(*a*) the public body that is storing the electronic data grants permission to the person; and
(*b*) in the case of personal data of an individual, in addition to permission under Paragraph (*a*), the individual whose personal data is being requested, has given his written consent.

(3) A person requesting to obtain electronic data stored in the Central Electronic Data Repository must apply in writing for permission to the public body that stored the electronic data.

(4) Permission granted under Subsection (3), must be in writing and must specify -
(*a*) the reasons for granting access; and
(*b*) the type of electronic data that will be accessed or shared; and
(*c*) the time period allowed to access the electronic data; and
(*d*) any other requirements that the person requesting access needs to observe.

(5) If electronic data stored in the Central Electronic Data Repository is classified as top-secret data or confidential data, regulation and standards may prescribe additional requirements for access to such data and restrictions on how that data may be used.

(6) Physical access to the Central Electronic Data Repository by any person must comply with security standards and specifications.

(7) Nothing in this section prevents or limits an individual from obtaining his personal data stored in the Central Electronic Data Repository if he verifies and authenticates his identification to be the person whose personal data is being stored.

(8) Nothing in this section prevents or limits a Department responsible for ICT matters, national planning matters, national budget matters and finance matters from obtaining data stored in the Electronic Data Repository for the purposes of national planning or national budget.

(9) For the purposes of Subsection (8), the Departmental Head shall ensure data is anonymised before it is obtained.

30. REDUNDANCY FOR CENTRAL ELECTRONIC DATA REPOSITORY.

(1) In addition to the Central Electronic Data Repository, the Department is to have one or more other data centres, for electronic data backup storage and electronic data redundancy.

(2) Each of the additional data centres must -

(*a*) have a daily synchronisation with the Central Electronic Data Repository; and

(*b*) meet the cyber security standards under this Act; and

(*c*) have a transmitter connecting it to the Central Electronic Data Repository.

31. SECURED DATA EXCHANGE PLATFORM.

(1) The Department shall develop, operate and maintain a secured data exchange platform for all public bodies.

(2) The secured data exchange shall -

(*a*) provide security for all government data stored or shared for digital service deliver; and

(*b*) facilitate sharing of data amongst public bodies' systems to deliver digital services in an effective manner.

(3) Any government sanctioned digital identity verification and authentication service must be secured by the secured data exchange.

(4) Secured API shall be used to facilitate data exchange for digital identity verification and authentication services.

(5) This section takes effect on the date the secured data exchange is made operational and published in the National Gazette.

32. PHYSICAL SECURITY SURVEILLANCE USING DIGITAL TECHNOLOGY.

(1) Without prejudice to any other law, a person using or proposing to use digital infrastructure or ICT to provide static, aerial or underwater physical security surveillance and monitoring services to the premises or property of a public body, shall comply with the standards and specifications under this Act.

(2) For the purpose of Subsection (1), physical security surveillance and monitoring services using digital infrastructure or ICT includes the following:

(*a*) static and mobile cameras; and

(*b*) aerial drones; and

(*c*) underwater drones; and

(*d*) geographical positioning hardware and software; and

(*e*) all other ICT instruments, equipment, devices and apparatus capable of being used to conduct physical area security surveillance to collect electronic data.

(3) A person providing services under Subsection (1) must make available data in electronic form collected to the public body.

PART IV. - DIGITAL SERVICES AND RELATED MATTERS.

33. DIGITAL SERVICES.

(1) Public bodies may provide digital services through the internet or shared services, that may include -

(*a*) applications, registrations, reporting, monitoring, renewals, evaluation and payments; and
(*b*) any government-to-citizen digital services; and
(*c*) any government-to-business digital services; and
(*d*) any government-to-government digital services; and
(*e*) any other services delivered or accessed using the internet system.

(2) For the avoidance of doubt, a service referred to in Subsection (1), may also be a digital infrastructure if the service is packaged under a platform as a service or a software as a service.

34. PROVISION AND ACCESSIBILITY OF DIGITAL SERVICES.

(1) If a public body provides a service, the public body may do all or any of the following:
(*a*) make the service accessible as a digital service; or
(*b*) deal with any data, information or documents relating to the service in electronic form.

(2) A public body in making accessible digital services must -
(*a*) use one or more systems; and
(*b*) use open APIs, closed APIs or hybrid APIs appropriate in the circumstances; and
(*c*) ensure its business processes enhance digital services; and
(*d*) use appropriate channels, documentation and languages, both spoken and sign, and use audible instructions if necessary; and
(*e*) ensure accessibility to people with disabilities and people with limited access to electronic services; and
(*f*) ensure audio and video formats are captioned for people with disabilities; and
(*g*) ensure adequate system support for all users; and
(*h*) maintain and promote integrated, interoperable and transparent and accountable systems; and
(*i*) comply with any other requirements prescribed by the standards and regulations made under this Act.

(3) A public body may provide a digital service or make a digital service accessible in all or any of the following forms:
(*a*) word document soft copy form; or
(*b*) photographic image that is accurately described in the alternative text of a document, website, or other online or electronic location and provided in a soft copy form; or
(*c*) digital audio or video form that is captioned and accessible to people with disabilities; or
(*d*) any other electronic form or expression easily accessible by people with disabilities; or
(*e*) any other sign, signal or expression in soft copy.

(4) The Department may issue standards, specifications and guidelines not inconsistent with this Act for providing digital services or making digital services accessible.

35. NATIONAL E-GOVERNMENT ONLINE PORTAL.

(1) The Department shall establish a National e-Government Online Portal for public bodies to deliver digital services.

(2) The National e-Government Online Portal shall -

(*a*) facilitate a centralised approach and provide seamless access to all digital services; and

(*b*) provide shared digital services to public bodies; and

(*c*) enable government to citizen -

(i) electronic authorisation for validation and updating of personal data; and

(ii) electronic access by a citizen to his personal data; and

(iii) electronic receipt of payment services; and

(iv) electronic payment services options; and

(v) electronic monitoring and tracking of service payment status; and

(*d*) enable government to government -

(i) electronic reporting modules for government revenue; and

(ii) electronic interface for government central agencies; and

(iii) other government e-business requirements.

(3) Subject to Subsection (4), the Department is to be the only provider of the National e-Government Online Portal.

(4) The Departmental Head may, acting on the recommendation of the ICT Steering Committee, outsource the management of the National e-Government Online Portal in part or in whole.

36. OPEN DATA.

(1) When developing open government data principles, the Department shall have regard to the following:

(*a*) the potential risk on government for the use of open data; and

(*b*) public use of data to contribute to innovation and productivity across all sectors of the economy; and

(*c*) quality of free and easy to use data; and

(*d*) data source and availability for use by the public, industry and academia; and

(*e*) availability of non-sensitive publicly funded research data for use and reuse; and

(*f*) availability and use of specialised data services; and

(*g*) security of open data sharing and integration; and

(*h*) open data use by local and provincial governments; and

(*i*) standards of security and privacy for individuals, national security and commercial confidentiality; and

(*j*) use of systems to support discoverability, interoperability, data and information accessibility; and

(*k*) any other matters prescribed by the standards.

(2) In making open data accessible, public bodies shall have regard to the following measures:

(*a*) to ensure that any open data is easily discoverable and available; and

(*b*) to ensure that any open data is in a machine-readable, spatially-enabled format; and

(*c*) to ensure that any open data contains descriptive information about what is included in the data; and

(*d*) to ensure that any open data is kept up to date in an automated way; and

(*e*) to ensure that any open data is of high quality, user-friendly and free API access.

37. SHARED SERVICES.

(1) For the purpose of public bodies providing digital services and making digital services accessible, shared services managed by the Department or any public body may consist of -

(*a*) shared services from the cloud infrastructure; and

(*b*) shared services from the digital infrastructure; and

(*c*) shared services amongst one or more departments or public bodies' networks.

(2) For the purpose of Subsection (1), shared services from -

(*a*) cloud infrastructure either lease or private government owned are digital services from one web hosting server used to host multiple clients with multiple websites or web applications; and

(*b*) digital infrastructure are ICT support skill resources and physical digital infrastructure resources.

(3) A public body hosting and using shared services is responsible for its local digital infrastructure within the Government Cloud Infrastructure.

(4) The Departmental Head may, in writing, declare any digital infrastructure to be a shared service for all public bodies.

(5) Upon declaration of a shared service, all public bodies are to be given a reasonable period determined by the Secretary in which to commence use of the shared service.

(6) Before the declaration of a shared service, the Department may undertake an assessment to ensure the proposed shared service -

(*a*) enables public bodies to focus on their core duties; and

(*b*) achieves lower cost and economies of scale; and

(*c*) improves user experience; and

(*d*) reduces technology footprint, maintenance and security vulnerability; and

(*e*) addresses legacy system issues; and

(*f*) satisfies other criteria determined by the Departmental Head.

(7) A public body shall not develop, maintain or use any service that the Departmental Head has determined is -

(*a*) standalone to a declared shared service; or

(*b*) a duplicate of, or similar to, a declared shared service.

(8) Shared services must comply with the Regulations, standards and specifications.

38. GOVERNMENT DOMAIN.

(1) Subject to Subsection (3), the Department is to manage the government domain.

(2) All public bodies must use the government domain for official purposes.

(3) The Department may outsource the registration and management of the government domain to a person qualified to manage domain name services.

(4) The Department is to establish and keep up to date a register of government domain names of public bodies, which must be publicised on the Department's website.

39. GOVERNMENT EMAILS.

(1) A public body must use the government domain as the email domain for all official emails of the public body.

(2) Subject to Subsection (3), a public body that uses an email domain that is not the government domain, any such email is not an official email of the public body.

(3) If, during a specific period, it is not practicable for a public body to use the government domain as the public body's email domain, the public body must, on the day it is not practicable to use the government domain, apply in writing to the Departmental Head for permission to use another email domain.

(4) Permission granted under Subsection (3) must specify the -

(*a*) email domain to be used; and

(*b*) period the email domain or website domain may be used.

(5) A person who, does not use the government email domain in his official capacity for government business correspondence, is guilty of an offence.

Penalty: A fine not exceeding K5,000.00 or imprisonment for a period not exceeding 12 months, or both.

40. GOVERNMENT WEBSITES.

(1) A public body must use the government domain as the website domain for all official websites of the public body.

(2) Where a public body uses a website domain that is not the government domain, any such website is not an official website of the public body, unless the Secretary has granted permission under Subsection (7).

(3) An official website of a public body must -

(*a*) contain functional links of other relevant public bodies located on a place approved by the Department on the website; and

(*b*) use text format approved by the Department; and

(*c*) contain correct information about the organisational structure and mandate of the public body; and

(*d*) ensure access to the webpage is mobile device friendly and be certified by the Secretary or by a person specialising in the field of digital accessibility, recommended by the Department; and

(*e*) ensure videos and multimedia files uploaded and available on the website -

(i) are captioned and accessible to people with disabilities; and

(ii) do not automatically play when a person accesses a webpage; and

(iii) use as little bandwidth capacity as practicable; and

(*f*) contain links to information about the public body's -

(i) privacy policy; and

(ii) point of contact; and

(iii) open data; and

(iv) be easy to navigate to obtain relevant information; and

(*g*) strategic plan and annual performance plan.

(4) Digital content that is developed, maintained or owned by a public body must be accessible on an official website of the public body, and may include all or any of the following:

(*a*) digital services; or
(*b*) sector specific guidance that aligns with a government policy intent linked to user needs; or
(*c*) policy and consultation documents for good governance; or
(*d*) published guides on laws and regulations and other subordinate instruments; or
(*e*) information on government services; or
(*f*) information on business opportunities; or
(*g*) awareness-raising campaigns and templates.

(5) The Departmental Head or his delegate, shall cause to be physically or virtually removed from the Internet a public body's website that does not comply with this section.

(6) Before taking action under Subsection (5), the Departmental Head shall give the public body 30 days to rectify.

(7) If, during a specific period, it is not practicable for a public body to use the government domain as the public body's website domain, the public body must, as soon as practicable, apply in writing to the Secretary for permission to use another website domain.

(8) Permission granted under Subsection (7) must specify the -

(*a*) website domain to be used; and
(*b*) period the website domain may be used.

(9) Unless permission is granted under Subsection (7), if a person responsible for facilitating use of government website domain of a public body, fails to facilitate use of the government domain by that public body, the person is guilty of an offence.

Penalty: A fine not exceeding K5,000.00 or imprisonment for a period not exceeding 12 months, or both.

41. GOVERNMENT SOCIAL MEDIA ACCOUNTS.

(1) The Department shall regulate the social media accounts of public bodies through standards, guidelines and specifications.

(2) A public body shall not operate a social media account online without approval from the Secretary.

(3) A public body shall inform the Departmental Head of the social media accounts details, including the purposes for the account and the proposed time period for its use.

(4) The Department shall facilitate the coordination, standardisation and streamlining of official government information disseminated on the social media accounts of public bodies.

(5) If, a National Event is being broadcasted, the Department reserves the right to broadcast that National Event on any social media accounts of a public body.

(6) Content published on social media accounts of public bodies is deemed to be official government information and must be stored as back up in the Central Electronic Data Repository.

(7) The Department shall establish a register of social media accounts of public bodies, keep the register up to date, and publish the register on the Department's website.

(8) The Department shall physically or virtually remove from the Internet any social media account of a public body that does not comply with any of the standards or specifications.

(9) Before taking action under Subsection (7), the Department shall give the public body 30 days to remove or rectify the social media account.

(10) A person who creates a social media account purporting to be an official social media account of a public body, and the social media account so created is not an official social media account of the public body, the person is guilty an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K10,000.00 or imprisonment for a period not exceeding 12 months, or both; and
(*b*) In the case of an offence by a body corporate, a fine not exceeding K50,000.00.

(11) A person who knowingly disseminates information purporting to be from an official social media account of a public body, and the social media account is not an official social media account of the public body, the person is guilty of an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K10,000.00 or imprisonment for a period not exceeding 12 months, or both; and
(*b*) In the case of an offence by a body corporate, a fine not exceeding K50,000.00.

(12) To avoid doubt, an official social media account of a public body is not required to use the government domain.

(13) For the purposes of administrating this section, the Departmental Head, by force of this law, is the co-admin of all public bodies' social media accounts.

42. MOVING TO PAPERLESS.

The Department is to develop regulation, standards, specifications and guidelines on paper reduction made under Section 64, while having regard to the following:

(*a*) the use of electronic identification of public officers and software-based document management systems; and
(*b*) electronic filing of paper-based records; and
(*c*) reduce reliance on excessive printing of documents; and
(*d*) use of electronic forms and online or cloud storage; and
(*e*) electronic note taking and reporting; and
(*f*) assist public bodies digitalised manual process.

43. ICT INCUBATION HUB.

(1) The Department may provide technical and administrative support to a public body that is responsible for administering ICT innovation, research and development initiatives.

(2) In the absence of a public body under Subsection (1), the Department may, act as the public body responsible for administering ICT innovation, research and development initiatives.

(3) The Department as the agent of the State is indemnified from any liability for works done by participants or services rendered to the participants of the ICT incubation hub under this section.

(4) The establishment of an ICT incubation hub does not prevent any person from discharging functions similar to the functions of such a hub under this section.

PART V. - ELECTRONIC DATA.

44. ELECTRONIC DATA GOVERNANCE ACROSS GOVERNMENT.

(1) For the purposes of this part, reference to electronic data governance applies to the whole of government data-value cycle process of data generation, collection, processing, storage, use and sharing of electronic data by public bodies.

(2) The Department must -

(*a*) build capacity for the implementation of electronic data governance measures; and

(*b*) provide oversight on electronic data infrastructure, such as data register, APIs, cloud-based solutions and other infrastructure related to electronic data governance; and

(*c*) manage electronic data architecture, including interoperability, integration, reference data, schematics and data relationship; and

(*d*) manage data-value cycle described in Subsection (1).

45. CLASSIFICATIONS OF ELECTRONIC DATA.

(1) Electronic data shall be classified under a regulation as -

(*a*) top-secret data if the unauthorised use, disclosure, alteration or destruction of the data results in a significant level of risk to the government; or

(*b*) confidential data if the unauthorised use, disclosure, alteration or destruction of the data results in a moderate level of risk to the government; or

(*c*) open data if the unauthorised use, disclosure, alteration or destruction of the data may result in little or no risk to the government.

(2) Standards made under Section 64 is to prescribe security controls to be applied by public bodies for safeguarding electronic data against unauthorised use, disclosure, modification or destruction having regard to the classifications of data referred to in Subsection (1).

46. REPRODUCTION, ETC., OF ELECTRONIC DATA.

(1) Any electronic data that is classified as top-secret data must not be stored, reproduced, altered, modified, disseminated or used by a person, unless that person is permitted by law.

(2) A person who, without lawful authority, accesses, uses, reproduces or disseminates electronic data that is classified as top-secret data under the regulations, is guilty of an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K100,000.00 or imprisonment for a period not exceeding 20 years, or both; and

(*b*) In the case of an offence by a body corporate, a fine not exceeding K1,000,000.00.

(3) A person who, without lawful authority, accesses, uses, reproduces or disseminates electronic data that is classified as confidential data under the regulations, is guilty of an offence.

Penalty: (*a*) in the case of an offence by a natural person, a fine not exceeding K100,000.00 or imprisonment for a period not exceeding five years, or both; and
(*b*) in the case of an offence by a body corporate, a fine not exceeding K500,000.00.

47. PUBLIC ACCESS TO ELECTRONIC DATA.

(1) For the purposes of this section, "access" means the generation, collection, procession, storage, usage and sharing of electronic data.

(2) Notwithstanding any other law, a public body shall manage access to electronic data in accordance with this Act.

(3) A person shall not access any electronic data stored by a public body, unless -
(*a*) the public body grants permission; and
(*b*) in the case of personal data of an individual, in addition to permission under Paragraph (*a*), the individual whose personal data is being stored by electronic means by a public body, gives his written consent.

(4) A person must apply in writing to the public body for permission.

(5) Permission granted by a public body must be in writing and must specify -
(*a*) the reasons for granting access; and
(*b*) the type of electronic data that will be accessed; and
(*c*) the time period allowed for the electronic data access; and
(*d*) all other requirements that the person requesting access needs to observe.

(6) Nothing in this section prevents or limits an individual from accessing his personal data stored by a public body.

(7) This section does not apply to open data that is made available to a public body through any electronic means under Section 36.

48. ELECTRONIC DATA COLLECTION AND STORAGE.

(1) Subject to Subsection (2), a public body must collect and store data in electronic form.

(2) On and after a date declared in writing by the Departmental Head, a public body in performing its functions must ensure that data is -
(*a*) collected in electronic form at its first point of collection; and
(*b*) subsequently stored in electronic form in accordance with the regulations and standards.

(3) Electronic data shall be collected and stored by utilising any electronic device capable of collecting, processing and storing data in accordance with the regulation and standards made under this Act.

(4) The Department is to be responsible for the oversight of electronic data collection and storage by public bodies, including when a public body converts any data collected in non-electronic form into electronic form.

49. OWNERSHIP OF ELECTRONIC DATA IN CENTRAL ELECTRONIC DATA REPOSITORY.

(1) Where -

(*a*) a public body has a right of ownership to electronic data; and

(*b*) that data is stored as backup in the Central Electronic Data Repository,

that electronic data stored as a back-up is the property of the State.

(2) For the avoidance of doubt, Subsection (1) extends to electronic data that is collected and stored by a person engaged by a public body under a contract or agreement.

(3) A public body who collects and stores or engages another person to collect and store data in electronic form, upon settlement of any contract fees, the public body must -

(*a*) have full access and control of the data collected and stored; and

(*b*) ensure the data collected and stored is backed up as storage in the electronic data repository.

(4) A person engage under Subsection (3), must take all reasonable steps, to provide the data in a mutually agreed format and means to the public body first mentioned.

(5) A person who, contravenes Subsection (3), is guilty of an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K100,000.00 or imprisonment for a period not exceeding 12 months, or both; and

(*b*) In the case of an offence by a body corporate, a fine not exceeding K1,000,000.00.

50. ELECTRONIC SYSTEMS INTEGRATION.

(1) A public body must comply with the standards and specifications for electronic system integration.

(2) Subject to Subsection (3), the electronic system integration standards and specifications must -

(*a*) prescribe matters relating to the use of APIs to share electronic data for digital service delivery; and

(*b*) prescribe matters relating to specifications of APIs that are -

(i) machine readable; and

(ii) publicly accessible; and

(iii) stable and scalable; and

(iv) available to other public bodies; and

(v) able to function on different platforms using multiple languages; and

(vi) be consistent with government policy on cyber security.

(3) API used by a public body to enable access to open data in Section 36 must -

(*a*) be properly documented with sample code and sufficient information for developers to make use of, if appropriate; and

(*b*) have their life-cycle made available by the public body owning it, if appropriate; and

(*c*) be backward compatible with at least two earlier versions; and

(*d*) enable a public body, if appropriate, to use an authentication mechanism to enable service interoperability on a single sign-on system; and

(*e*) promote easy and transparent integration and interoperability of electronic data; and

(*f*) promote safe and reliable sharing of electronic data and information to enable delivery of digital services; and
(*g*) encourage and enable innovation; and
(*h*) promote open standards of software interoperability across public bodies; and
(*i*) ensure easy access of information collected by public bodies; and
(*j*) comply with any other requirements prescribed by the standards and specifications.

(4) A public body using one or more systems shall make available to the Department the specifications of the APIs used by the public body to deliver digital services.

(5) The Department shall establish and maintain a register of APIs used by public bodies.

(6) The Departmental Head is to issue API standards for different digital infrastructure levels, application level, network level and server level to govern the flow of government electronic data.

51. ELECTRONIC DATA REGISTER.

(1) The Department shall establish and maintain an Electronic Data Register.

(2) The Electronic Data Register shall contain a record of the types of electronic data collected, stored and shared by public bodies.

(3) The Electronic Data Register may be used for cataloguing electronic data collected, stored and shared by public bodies.

52. ELECTRONIC DATA SHARING.

(1) A public body must comply with the standards and specifications for electronic data sharing.

(2) When sharing electronic data, a public body must take the necessary precautions to ensure that the sharing of the data is done in a secured manner without causing data privacy violations or leaving the data open to being hacked.

(3) For the purpose of facilitating data sharing across government, the Department is to establish and use the secured data exchange.

53. ELECTRONIC DATA IN PROVINCES AND DISTRICTS.

The Department, in the discharge of its functions under this Act, must take reasonable steps to collaborate with any other public body mandated by law to deliver services in provinces and districts with respect to the generation, collection, processing, storing, securing, using and sharing of electronic data.

PART VI. - ENFORCEMENT.

54. NOTICES.

The Departmental Head may issue notices under this part in the prescribed form.

55. DIRECTIONS.

(1) The Departmental Head may, acting on advice of the NEC, not inconsistent with the provisions of this Act or other laws, issue all or any of the following directives to an internet service provider or any other person providing internet services or a platform as a service to a public body:
(*a*) to deploy NCSC approved technology for cyber safety and security; or
(*b*) to prohibit or restrict the use of a software application in Papua New Guinea that poses a serious risk or threat to public health, safety, welfare or national security; or

(*c*) if there is considered to be a serious risk or threat to public health, safety, welfare or national security, to do all or any of the following:
  (i) shut a website down; or
  (ii) filter, restrict or otherwise modify the operation of a website so that it cannot be used; or
  (iii) monitor and control the content of a website; or
  (iv) control expressions on a website by blocking, keyword filtering or censoring the website; or
  (v) cancel or suspend social media platforms; or
  (vi) restrict or lock access to specific internet protocol addresses; or

(*d*) require all video sharing platforms to -
  (i) have fake video detector capability; and
  (ii) enable users of those platforms to check and report fake videos and audios.

(2) A direction under subsection (1), shall take effect on the day, the Minister acting with, and in accordance with the advice of the NEC, publish a notice in the National Gazette.

(3) A person who, without lawful authority, contravenes or fails to comply with a direction, is guilty of an offence -

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K50,000.00 or imprisonment for a period not exceeding five years, or both; and
(*b*) In the case of an offence by a body corporate, a fine not exceeding K500,000.00.

(4) The Departmental Head may make standards for the purposes of Subsection (1).

56. ACCESS TO SYSTEMS, INVESTIGATION, ETC.

(1) For the purpose of performing its functions under this Act, the Departmental Head may -
(*a*) direct a public body to give the Department physical or virtual access to a system of the public body; and
(*b*) direct a public body to cease using a private network that is not consistent with this Act, the regulations, standards or specifications; and
(*c*) direct a public body to give the Department access to any source data of any format from the public body; and
(*d*) receive, investigate, respond to and publish complaints relating to digital services provided by a public body; and
(*e*) stop or suspend the implementation of any ICT project, digital services project or digital infrastructure project by a public body that is not in compliance with the regulations, standards or specifications; and
(*f*) direct any public body to -
  (i) furnish any information or produce any record or document relating to ICT projects, digital services or digital infrastructure; and
  (ii) answer all relevant questions relating to digital government initiatives; and
(*g*) examine any records or documents of a public body relating to ICT projects, digital services or digital infrastructure and take copies or extracts; and
(*h*) power to do all things necessary or convenient to be done for or in connection with the performance of the Department's functions.

(2) A direction under Subsection (1)(*a*), (*b*), (*c*) or (*f*) must be in writing.

57. POWERS OF OFFICERS OF THE DEPARTMENT.

A Department officer has, in carrying out enforcement actions under this Part, powers to do all or any of the following:

(*a*) enter and search a premises or system to ascertain whether non-compliance with this Act has occurred; or

(*b*) interview a person where the officer believes, on reasonable grounds, that he has knowledge or information regarding non-compliance with this Act; or

(*c*) require a person to provide information pertaining to non-compliance with this Act; or

(*d*) seize any items related to a breach of this Act.

PART VII. - OFFENCES.

58. OFFENCES.

(1) A person who, intentionally and without lawful authority -

(*a*) accesses, uses, reproduces or disseminates electronic data in the course of the person's employment or engagement with a public body; or

(*b*) accesses, uses or reproduces electronic data from a public body's system or digital infrastructure; or

(*c*) disseminates electronic data of a public body or transmits electronic data of a public body through unauthorised channels; or

(*d*) removes, destroys, alters or damages electronic data of a public body; or

(*e*) removes, destroys, alters or damages critical digital infrastructure or a public body's digital infrastructure, software, hardware or system,

is guilty of an offence.

Penalty: (*a*) In the case of an offence under Subsection (1)(*a*), (*b*) or (*c*) -

(i) for a natural person, a fine not exceeding K20,000.00 or imprisonment for a period not exceeding 5 years, or both; and

(ii) for a body corporate, a fine not exceeding K100,000.00; and

(*b*) In the case of an offence under Subsection (1)(*d*) or (*e*) -

(i) for a natural person, a fine not exceeding K100,000.00 or imprisonment for a period not exceeding 10 years or both; and

(ii) for a body corporate, a fine not exceeding K500,000.00.

(2) Subsection (1) does not apply to open data.

(3) A person who fails to comply with a provision of this Act for which no specific penalty is provided, is guilty of an offence.

Penalty: (*a*) In the case of an offence by a natural person, a fine not exceeding K5,000.00, or imprisonment for a period not exceeding 12 months, or both; and

(*b*) In the case of an offence by a body corporate, a fine not exceeding K10,000.00.

59. MATTERS RELATING TO OFFENCES.

(1) The imposition of a penalty under this Act does not prevent -

(*a*) disciplinary action, whether under legislation, a contract or otherwise, also being taken against an individual, including termination of employment; or

(*b*) the cancellation or suspension of a person's operational licence, permit, approval or certificate under any other law.

(2) If a person is convicted of an offence under this Act, a court may, in addition to any penalties prescribed in this Act, order that the person convicted of the offence be required to pay to the State a sum equal to the cost of repairing any damage resulting from the commission of the offence.

(3) For the purpose of prosecuting an offence under this Act, an act or omission of an employee or agent of a body corporate is deemed to be an act or omission of the body corporate.

(4) For the purpose of public service disciplinary measures, if a public officer is suspended for an alleged offence under this Act, the offence is deemed to be an offence to which suspension with pay measures under the ***Public Services (Management) Act*** **1995** apply.

(5) The Department in consultation with the Department responsible for personnel matters may provide technical assistance to develop public service disciplinary procedures for offences under this Act.

(6) In enforcing this Act, the Department may refer any complaint, criminal or otherwise, relating to an offence under this Act to any lawful authority for prosecution.

60. PROSECUTION OF CRIMINAL OFFENCES.

A criminal offence against this Act shall be -

(*a*) prosecuted by the Department, if the offence is a summary offence; or

(*b*) prosecuted by the Public Prosecutor where the offence is an indictable offence.

PART VIII. - MISCELLANEOUS.

61. NEW COMMITTEES.

(1) The Department may form committees for the purposes of this Act and prescribe their terms of reference.

(2) A committee shall regulate the conduct of proceedings at its meetings as it thinks fit.

62. IMMUNITY.

A person engaged in the administration or enforcement of this Act is not personally liable (either civilly or criminally) for anything done or omitted to be done in good faith in the course of exercising their powers or carrying out duties under this Act.

63. REGULATIONS.

The Head of State, acting on advice from the National Executive Council, may make regulations not inconsistent with this Act, prescribing all matters provided for under this Act.

64. STANDARDS, SPECIFICATIONS, GUIDELINES OR CODES OF PRACTICE, ETC.

(1) The Department must make or may adopt standards, specifications, guidelines or codes of practice as necessary, for the effective implementation of this Act.

(2) The standards, specifications, guidelines or codes of practice adopted by the Department under Subsection (1) shall be published in the National Gazette.

65. SAVING AND TRANSITIONAL.

(1) Any contract or agreement between a public body and an ICT service provider, to the extent that they were in effect immediately before the coming into operation of this Act, are saved and continue to be valid as if made under this Act, until they expire or are terminated in accordance with law.

(2) A public body must, within three years of the commencement of this Act, make the necessary arrangements and transition for the purpose of complying with the requirements under this Act.

(3) Where a public body has been operating a social media account immediately before the commencement of this Act, the public body must, within 60 days after the commencement, notify the Department in writing of the details of the account.

(4) Subject to Subsection (5), where a private network of a public body is in operation immediately before the commencement of this Act, that private network is to, upon the commencement of this Act, be deemed to be a private network approved by the Secretary.

(5) If the Departmental Head determines, upon advice of the ICT Steering Committee, that the private network of the public body does not comply with this Act, the Departmental Head shall issue the appropriate notice in writing, directing the public body to comply with the requirements of this Act.

(6) Upon receiving a notice under Subsection (5), a public body shall cease to use the private network or make a written request to the Department to use the private network.

(7) Upon receipt of a request under Subsection (6), the Department shall refer the request to the ICT Steering Committee for consideration to make the appropriate recommendation to the Departmental Head.

(8) The Departmental Head shall, on the recommendation of the ICT Steering Committee, reject or approve the request in writing, subject to conditions (if any) as determined by the Departmental Head.

(9) If a request by a public body is rejected pursuant to Subsection (8), the public body must cease to use the private network within 60 days of receipt of the notice.

(10) If a public body, immediately before the commencement of this Act, is not using the government domain as its email domain, the public body shall, within one year of commencement of this Act, work with the Department to use the government domain as the public body's email domain.

(11) If a public body, immediately before the commencement of this Act, is not using the government domain as its website domain, the public body shall, within one year of the commencement of this Act, publish online its website ending in the government domain.

(12) A public body that fails to comply with Subsections (10) or (11) commits an offence.

(13) A person conducting ICT business with a public body under a contract or agreement to which this section applies, has 3 years from the commencement of this Act, to ensure the services provided to the public body under the contract or agreement comply with this Act and the regulations, standards and specifications.

(14) A person who, fails to comply with Subsections (13), is guilty of an offence.

Penalty: A fine not exceeding K1,000,000.00, or imprisonment for a term not exceeding seven years, or both.

I hereby certify that the above is a fair print of the ***Digital Government Act* 2022**, which has been made by the National Parliament.

Clerk of the National Parliament.
19 JUL 2022

I hereby certify that the ***Digital Government Act* 2022**, was made by the National Parliament on 21 April 2022, by an absolute majority in accordance with the ***Constitution***.

Speaker of the National Parliament.
19 JUL 2022