REPUBLIC OF KIRIBATI

Arrangement of Sections

PART I
PRELIMINARY

PART II
ADMINISTRATION

Division 1- General Administration

Division 2- ICT Practitioners

Division 3- Board and Committees

Division 4- National Computer Emergency Response Team

PART III
DIGITAL INFRASTRUCTURE

PART IV
DIGITAL SERVICES AND RELATED MATTERS

PART V
COMPUTER DATA

PART VI
ENFORCEMENT

THE REPUBLIC OF KIRIBATI

(No.____ of 2023)

I assent

_____

Beretitenti
_____2023

A Bill

entitled

AN ACT TO PROVIDE FOR DIGITAL GOVERNMENT THROUGH THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES ACROSS THE WHOLE OF GOVERNMENT DIGITAL SERVICES, DIGITAL INFRASTRUCTURE, DIGITAL SKILLS AND FOR OTHER RELATED DIGITAL GOVERNMENT PURPOSES;

Commencement date:

_____2023

MADE by the Maneaba ni Maungatabu and assented to by the Beretitenti.

PART I
PRELIMINARY

1. Short title
This Act shall be cited as the ***DIGITAL GOVERNMENT ACT 2023***.

2. Principles of implementation of Digital Government
In implementing this Act, the Government and the people should be able to understand the following underlying principles:

(1) Digital government is about government processes and operations in relation to digital services and technologies rather than just digital presence;
(2) Digital government promotes causes of e-citizen and e-democracy;
(3) Digital government services should be accessible to all;
(4) Digital government is an integrated government systems;
(5) Digital government prefers open sources to proprietary software; and
(6) Digital government expects cooperation between government ministries.

3. Compliance with Constitutional Requirements
This Act, to the extent that it regulates or restricts a right or freedom referred to in Chapter II of the Constitution, namely-

(1) the right to freedom of expression and information conferred by Section 12;
(2) the right to privacy conferred by Section 9; and
(3) the right to protection from unjust deprivation of property conferred by Section 8.

4. Interpretation
In this Act, unless the context requires:

“application” means a distinct set of machine instructions that are interpretable and executable by a computing device and designed to fulfill 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;
“Board” means the National Digital Transformation Advisory Board established under section 15;
“classification of computer data” means a computer data classified under section 45 as top-secret data, confidential data and open data;
“computer data” means any representation of fact, information or concept in a form suitable for possessing in a computer system, including a computer program suitable to cause a computer system to perform a function;
“cloud infrastructure” means the numerous data centers 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 under section 23;
“digital transformation office” or “DTO” means the division responsible for information and communications technology established under section 8;
“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 12;
“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 include, but is not limited to the following:

(a) the Government Computer Data Repository;
(b) data registers;
(c) ICT platforms;
(d) cloud infrastructure;
(e) the Government Cloud Infrastructure;
(f) the Government Private Network and other networks;
(g) systems;
(h) software applications;
(i) APIs and integration;
(j) Endpoint devices;
(k) Internet exchange points;
(l) Servers, routers and modems enabling system connectivity of virtual private network and wireless by-pass links; and
(m) Telecommunication infrastructures such as broadband, satellite connectivity, radio links, optic fiber, dark fiber, copper cables and all other related systems;

“digital services” means internet enabled services that are delivered and accessed using digital infrastructure;
“DTO officer“ means the DTO officers who has oversight of, and is responsible for ICT matters within the DTO or public bodies, and he is deemed to be a delegate of the SRO of a public body with respect to ICT matters;
“Director” means the director responsible for digital transformation office or “DTO” appointed under this Act to perform functions for the purpose of administering this Act;
“computer 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 delivering 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 machines- readable code or instructions;
“computer data register” means the computer 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 computer data repository” means the Government Computer Data Repository established under section 27 as the official storage server to backup computer data of public bodies and provide safety against potential unforeseen events that may cause data loss to public bodies;
“government domain” means the domain ending in gov.ki;
“government leased cloud infrastructure” means the cloud infrastructure owned by a cloud service vendor and used by the DTO 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;
“ICT” means information and communications technology;
“ICT audit committee” means the Public Service ICT Audit Committee established under section 18;
“ICT project design” means an ICT infrastructure plan of a public body to deliver digital Government;
“Minister” means the Minister responsible for ICT;
“Ministry” means the Ministry responsible for ICT;
“national computer security emergency response team “CERT” means the National computer emergency response team referred to in section 20;
“National Digital Government Portal” means the National Digital Government Portal established under section 33;
“Officer” means an officer or employee of the DTO;
“open data” means any government computer data that any person can access, use and share, and which is deemed to be a public data under section 34;
“public body” means the Government’s office including Island Councils, Judiciary and ‘te Maneaba ni Maungatabu but does not include State Owned Enterprises;
“Secretary” means the Secretary responsible for ICT;
“Senior Responsible Officer or SRO” means the head of public bodies;
“specialized data services” means tools or software for working with the data, such as data visualization software or machine learning algorithms. These services can be particularly useful for researchers, businesses, and organizations that require specialized data to support their work or decision-making;
“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 computer data to produce a specific output;
“system integration” means connecting one or more systems so that computer 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 computer data in real-time and use the date that has been exchanged;
“Top-secret data” has the meaning under section 45;

5. Objectives of the Act

This Act aims to-

(1) establish the Digital Transformation Office (DTO);

(2) outline functions or roles and responsibilities of DTO;

(3) establish ICT Advisory Board that will provide monitoring and evaluation for the Digital Government processes;

(4) establish the National Computer Emergency Response Team;

(5) establish the ICT Audit Committee;

(6) establish a composition of ICT Practitioners for the better coordination of ICT related matters and for the effectiveness and efficiency of Digital Government Development; and

(7) enforce and regulate the principles and guidelines stipulated under any Government Plans relevant to digital services and ICT.

6. Application

(1) This Act binds the Republic.

(2) This Act is not applicable to State-Owned Enterprises.

PART II
ADMINISTRATION

Division 1- General Administration

7. Administration of the Act

(1) This Act shall be administered under the direction and control of the Secretary.

(2) Any person who acts in any manner to breach any requirement imposed by the Secretary in the exercise of a function or power under the preceding subsections, commits an offence punishable under this Act.

8. Establishment of DTO

DTO is hereby established to perform and implement its functions under this Act.

9. Functions of DTO

(1) The DTO shall have the following functions;

(a) develop and update ICT policies;
(b) coordinate general operational matters relating to ICT for public bodies;
(c) coordinate the construction and delivery of whole of government digital infrastructure and digital services;
(d) support operations with agencies responsible for national intelligence and national security to ensure cyber security and safety are maintained across whole of government;
(e) establish and maintain a whole of government register of systems, digital infrastructure and digital services;
(f) develop and review plans as necessary for the purpose of delivering digital services; and
(g) ensure public bodies comply with this Act;
(h) institute proceedings for offences against this Act;
(i) perform such other functions conferred on the DTO by this Act, an instrument or any other law;
(j) approve procurement of ICT systems for all public bodies;
(k) coordinate postings and specialized training for DTO officers in consultation with SRO; and
(l) any other functions specified in the approved Digital Government Plan.

10. Powers of DTO

The DTO 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.

11. Delegation

The Director may delegate, in writing, to an officer of the DTO any of his powers or functions under this Act except for the power of delegation.

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

(2) The DTO 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 DTO officers.

12. Digital Government Plan

(1) The Director shall prepare the Digital Government plan in accordance with the advice of the National Digital Transformation Advisory Board and approved by Cabinet.

(2) The Director shall circulate the approved Digital Government Plan to all public bodies and all public bodies must comply with the Plan.

(3) The Director shall ensure that digital services are implemented in accordance with the Digital Government Plan.

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

(5) DTO Officers in consultation with their SRO shall, in accordance with the relevant guidelines, conduct an annual self-assessment of its implementation of the Digital Government Plan and submit the assessments to the Director on or before the end of the year to which the assessment relates.

Division 2- ICT Practitioners

13. ICT Practitioners

(1) There shall be a composition of ICT practitioners within the Ministry of which there shall be a position in respect of that composition in the Establishment Register.

(2) The Director is responsible for:

(a) determining the functions and roles of ICT practitioners with respect to section 14 for any position listed in the establishment register; and

(b) designating an appropriate officer to any public body upon written request of that body to execute the roles and responsibilities under section 14, as determined by the Director.

(3) The Director may mobilize ICT practitioners as the need arises to assist other public bodies in helpdesk and ICT technical support matters.

14. Roles and Responsibilities of ICT Practitioners

(1) The ICT Practitioners shall -

(a) coordinate with the DTO on ICT and Digital Transformation matter;

(b) facilitate integration and interoperability of the systems of the public body;

(c) facilitate delivery of digital services by the public body;

(d) manage the computer data in the public body;

(e) plan and prepare for approval of the annual ICT budget for the management of the ministry. The ICT budget should be in line with both the government ICT action plan and the ministerial action plan;

(f) cooperate with DTO in regard to implementation of different projects on public bodies and cross government level, supervision of projects, ICT training issues of ministries;
(g) organise ICT systems maintenance and user help desk;
(h) organise end user training on ICT issues; and

(i) provide ICT reports and feedback on a quarterly basis to the DTO or as requested by the Secretary.

Division 3: Board and Committees

15. Establishment of National Digital Transformation Advisory Board

The Board is hereby established.

16. Functions of the Board

The Board is responsible to:

(1) provide opinions and advice on basic and strategy issues on ICT;

(2) provide opinions and makes recommendations about ICT-related policy and legal issues; and

(3) monitor the progress of the implementation plan fulfillment semi-annually and give recommendations in case of deviations.

17. Members of Board

(1) Subject to section 15, the Board shall consist of:

(a) the Director of DTO as being Chairperson;
(b) a representative of the Public Service;
(c) a representative of Academic Institution;
(d) a representative of a Private Sector; and
(e) a representative from non governmental organisations

having the requisite expertise, social standing and professional ICT background appointed by the Minister.

(2) The Minister shall develop the rules and procedures of the Board meetings;

(3) At any meeting of the Board -
(a) 3 members of whom one is the Chairperson are quorum; and
(b) to convene twice a year or

(c) to call one special meeting if considered necessary by the Chairperson.

18. Public Service ICT Audit Committee

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

(2) The ICT Audit Committee shall consist of -

(a) any representative from the DTO nominated by the Secretary; and
(b) a representative of the Kiribati Audit Office nominated by the Auditor-General; and
(c) a Lawyer from the Office of the Attorney General nominated by the Attorney General; and
(d) a representative from the public body responsible for Finance nominated by the SRO; and
(e) a representative from the Public Service Office nominated by the SRO; and
(f) a representative from the Communications Commission of Kiribati appointed by Chief Executive Officer; and
(g) a representative of the non-government ICT Association.

(3) The Secretary shall determine the Chairperson of the Committee.

(4) The ICT Audit Committee shall;

a) meet if it considers necessary to assess and evaluate a public body's use of a system against regulations, standards or specifications under this Act;
b) the quorum shall be 4 of members; and
c) develop its own meeting rules and procedures

19. Functions of the ICT Audit Committee

(1) The ICT Audit Committee shall -

(a) perform ICT audits on the systems used by the public bodies at least once in a year; and
(b) perform other functions specified in the Committee's terms of reference as prescribed by the Secretary.

(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 organizational structure of the public body;
ii) the public body's internal ICT policies and procedures;
iii) the public body's compliance with this Act and the Regulations, standards and specifications;
iv) ICT documentation and ICT projects of the public body;
v) risk associated with the use of a system;

(b) interviewing the appropriate ICT personnel of the public body; and
(c) conducting such other audit activities as directed by the Director;
(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 Director.

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

Division 4 – National Computer Emergency Response Team

20. National Computer Emergency Response Team

(1) A National Computer Emergency Response Team (CERT) is hereby established within DTO.

(2) The DTO shall continue to provide administrative oversight of the CERT.

21. Functions of National Computer Emergency Response Team

(1) The National Computer Emergency Response Team shall coordinate all efforts and matter of national cyber security by performing the following functions:

(a) conduct defensive cyber security operations; and
(b) conduct cybersecurity awareness to the public; and
(c) promote a secure digital government environment; and
(d) ensure government digital infrastructure contains appropriate security control technologies; and

(e) promote cyber resilience to ensure services that are essential for everyday life remain effective and operational during cyber threats and attacks; and

(f) investigate any breaches of cyber security and escalate security incidents to appropriate authorities (if necessary), for their intervention; and

(g) monitor and hunt cyber threats across networks and end points, and ensure that threats attacking data and assets are contained and eliminated; and

(h) provide cyber incident response service to the Government, local businesses and the general public;

(i) conduct audits on cyber security tracking and monitoring systems and end point devices used by ministries; and

(j) establish procedures for the persons to whom the CERT provides services and other member organisations of the CERT to report cyber-attacks or suspected cyber incidents; and

(k) provide regular reports to the persons to whom the CERT provides services; and

(l) provide technical digital forensic support to the Kiribati Police Service's Cybercrime Unit; and

(m) recommend to the Director the prosecution of relevant offences; and

(n) perform other activities as directed in writing by the Director; and

(o) any other cyber security related functions specified by the Director.

(2) The Director may outsource all or any of the functions of the CERT.

PART III
DIGITAL INFRASTRUCTURE

22. Digital Infrastructure

The DTO shall coordinate the delivery of digital infrastructure that includes the critical infrastructure designated by the Minister under this Part.

23. Government Critical Digital Infrastructure

(1) The Government critical digital infrastructure is the digital infrastructure that is-

(a) owned by the State; or

(b) owned by a person, other than the State and used by public bodies under a software as a service arrangement or any other agreement;

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) Government Computer Data Repository;
(b) subject to subsection (1), Government Secure Network; and
(c) secure Data Exchange Platform

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

(4) The Government 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 decision of the Board.

24. Government Secure Network

(1) A Government Secure Network is hereby established.

(2) The Government Secure Network by the DTO and is to consist of the following-

(a) the Government Computer Data Repository;
(b) any physical, virtual or cloud networks connectivity operated, managed and utilized by the State; and
(c) digital infrastructure, internet, and software as services to enhance network connectivity and computer data sharing amongst public bodies.

(3) For the avoidance of doubt, the network in subsection (2) (b), does not preclude any portions or parts of the network infrastructure utilized by a public body that is owned by service providers to be subject to Regulations under the Communication Act 2013.

(4) All public bodies must use the Government Secure Network.

(5) The Government Secure Network shall be managed by the DTO in accordance with this Act.

25. Government Leased Cloud Infrastructure

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

(2) 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.

(3) A person who, whether under a contract or otherwise operates or facilitates operations of a ministry's cloud infrastructure outside of the Government Leased Cloud Infrastructure, commits an offence and is liable to a maximum fine of $10,000 or a maximum imprisonment for 5 years or both.

26. Government Private Cloud Infrastructure

(1) DTO shall build a Government Private Cloud Infrastructure as part of the Government Private Network for the delivery of digital services.

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

(3) The Government Private Cloud Infrastructure operational center is to be located in Kiribati.

(4) Any person who fails to comply with this section, commits an offence.

(5) This section takes effect on the date the Government Private Cloud Infrastructure is commissioned by the Director and subsequent notification to all public bodies.

27. Government Computer Data Repository

(1) The DTO shall establish and manage the Government Computer Data Repository.

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

(3) The Director may designate any storage system as part of the Government Computer Data Repository as the need arises.

(4) The Government Computer Data Repository must consist of the following:

(a) a physical computer data repository; and
(b) other redundancy data repositories established under section 30,
that are synchronized and operating as one data storage server for compulsory backup or redundant data storage for all public bodies.

28. Destruction of digital infrastructure

A person who, without lawful authority removes, destroys, alters or damages digital infrastructure or critical infrastructure or a public body's digital infrastructure

or hardware commits an offence and is liable to a maximum fine of $35,000 or a maximum imprisonment of 7 years or both.

29. Access to Government Computer Data Repository

(1) For the purpose of this section, access to the Government Computer Data Repository means access to different sections of the physical and virtual database servers consisting of:

(a) physical access to the holding vault of the main Government Computer Data Repository;
(b) physical and virtual access to the active operating system of the Government Computer Data Repository.

(2) Except for open data, a person shall not obtain any computer data stored in the Government Computer Data Repository unless-

(a) the SRO of the public body that is storing the computer data grants permission to the person;
(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 computer data stored in the Government Computer Data Repository must apply in writing for permission from the SRO of the public body that stored the computer data.

(4) Permission granted under subsection (3), must be in writing and must specify:

(a) the reasons for granting access;
(b) the type of computer data that will be accessed or shared;
(c) the time period allowed to access the computer data; and
(d) any other requirements that the person requesting access needs to observe.

(5) If computer data stored in the Government Computer Data Repository is classified as top-secret data or confidential data, regulations 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 Government Computer Data Repository by any person must comply with security standards and specifications.

(7) Any person found in contravention of the provisions under this part, commits an offence and shall be liable upon conviction under the provisions of the Cybercrime Act.

30. Redundancy for Government Computer Data Repository

(1) In addition to the Government Computer Data Repository, the DTO is to have one or more other data centers for computer data backup storage and computer data redundancy.

(2) Each of the additional data centers must:

(a) have a daily synchronization with the Government Computer Data Repository;
(b) meet the cyber security standards under this Act; and
(c) have a transmitter connecting it to the Government Computer Data Repository.

31. Secure data exchange platform

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

(2) The secure data exchange platform shall-

(a) provide security for all government data stored or shared for digital service delivery; 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 secure by the secure data exchange.

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

(5) This section takes effect on the date the secure data exchange platform is commissioned by the Director and subsequent notification to all public bodies.

PART IV
DIGITAL SERVICES AND RELATED MATTERS

32. Digital Services

(1) Public bodies may provide digital services through the internet that may include:

(a) applications, registrations, reporting, monitoring, renewals, evaluation and payments;
(b) any government-to-citizen digital services;
(c) any government-to-business digital services;
(d) any government-to-government digital services;
(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 software as a service.

33. National Digital Government Portal:

(1) The Director shall establish a National Digital Government Portal for public bodies to deliver digital services.

(2) The National Digital Government Portal shall:

(a) facilitate a centralized approach and provide seamless access to all digital services and information; and
(b) enable the government to citizen-

i) electronic access to Government digital services; and
ii) electronic authorization for validation and updating of personal data;
iii) electronic access by a citizen to his personal data;
iv) electronic receipt of payment services;
v) electronic payment services options; and
vi) electronic monitoring and tracking of service payment status.

(3) DTO is to be the only provider of the National Digital Government Portal.

34. Open Data

(1) When determining an open data, DTO shall have regard to the following:

(a) the potential risk on the government for the use of open data;
(b) public use of data to contribute to innovation and productivity across all sectors of the economy;
(c) quality of free and easy to use data;
(d) data source and availability for use by the public, industry and academia;
(e) availability of non-sensitive publicly funded research data for use and reuse;
(f) availability and use of specialized data services;

(g) security of open data sharing and integration;
(h) standards of security and privacy for individuals, national security and commercial confidentiality;
(i) use of systems to support discoverability, interoperability, data and information accessibility;
(j) 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;
(b) to ensure that any open data is in a machine-readable, spatially-enabled format;
(c) to ensure that any open data contains descriptive information about what is included in the data;
(d) to ensure that any open data is kept up to date in an automated way;
(e) to ensure that any open data is of high quality, user-friendly and free API access.

35. Approval for ICT aspects of project designs

(1) No public body shall adopt, purchase or use an ICT project design unless approved by the Director.

(2) Any public body who wishes to adopt, purchase, or use an ICT project design must request the Director in writing.

(3) Upon the receipt of the request under subsection (2), the Director must respond in writing within 30 days from the date of receipt or within such period extended by the Director in writing.

(4) The Director shall approve or reject an ICT project design of a public body based on the Digital Government Plan or relevant ICT sector plan, the ICT policies of the Government developed by DTO.

(5) If the DTO approves the ICT project design, the Director 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 Director rejects the ICT project design, he shall issue a written notice stating the reasons for rejection to the public body within 10 working days from the date of the decision.

(7) For the avoidance of doubt, this section applies to the approval of ICT project design before the procurement process under any law may take effect.

36. Certificate of Compliance for ICT project design

(1) This section applies to an ICT project design proposed by a public body where it requires-

(a) budget funding from the government; or
(b) donor funded projects.

(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 Finance department responsible for development budget matters and donor funding project;

(4) 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 donor funded projects.

(5) The SRO of a public body who fails to obtain a Certificate of Compliance before seeking funding under subsection (1), commits an offence punishable under this Act.

37. 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;
(b) deal with any data, information or documents relating to the service in electronic form.

(2) DTO in consultation with public bodies, in making accessible digital services shall:

(a) use one or more systems;
(b) use open APIs, closed APIs or hybrid APIs appropriate in the circumstances;
(c) ensure its business processes enhance digital services;

(d) use appropriate channels, documentation and take reasonable steps to convert English into Kiribati language, both spoken and sign, and use audible instructions if necessary;
(e) ensure accessibility to people with disabilities and people with limited access to electronic services;
(f) ensure audio and video formats are captioned for people with disabilities;
(g) ensure adequate system support for all users;
(h) maintain and promote integrated, interoperable and transparent and accountable system; and
(i) comply with any other requirements prescribed by the standards and regulations made under this Act.

(3) DTO may provide a digital service or make a digital service accessible in all or any of the following forms:

(a) electronic document;
(b) photographic image that is accurately described in the alternative text of a document;
(c) digital audio or video form that is captioned and accessible to people with disabilities;
(d) any other electronic form or expression easily accessible by people with disabilities;
(e) any other sign, signal or expression in soft copy.

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

38. Government Domain

(1) DTO shall be the registrar for the government domain .gov.ki and shall determine how the government domain is used in the government.

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

(3) DTO shall establish and keep up to date a register of government domain names of public bodies, which must be published on the government portal under section 33.

39. Government Emails

(1) All public bodies must use the government domain as the email domain for all official emails of the public body and must not be used for personal purposes.

(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 Director for permission to use another email domain.

(4) All public bodies must use multifactor authentication on emails used for official purposes or any other means that will strengthen the security of official emails.

(5) Permission granted under subsection (3) must specify-

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

(6) A person who does not use the government email domain in his official capacity for government business correspondence, is guilty of an offence and is liable to a maximum fine of $15,000.00 or maximum imprisonment of 3 years, 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 Director has granted permission.

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

(a) comply with standards or specifications developed by DTO;
(b) contain functional links of other relevant public bodies located in a place approved by DTO on the website;
(c) use text format approved by DTO
(d) ensure access to the webpage is mobile device friendly and be certified by the Secretary or by a person specializing in the field of digital accessibility and recommended by DTO.

(4) All public bodies shall publish on their official websites ;

(a) correct and updated information about the organizational structure and mandate of the public body;
(b) videos and multimedia files uploaded and available on the website-
i) are captioned and accessible to people with disabilities;

ii) use as little bandwidth capacity as practicable;

(c) contain information about the public body's-

i) privacy policy;

ii) point of contact;

iii) open data;

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

v) any other information the public body deems necessary for the use of the public.

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

(6) Before taking action under subsection (4), the Director shall give the public body three days to rectify.

(7) If a person responsible for facilitating the use of the government website domain of a public body, fails to facilitate the use of the government domain by that public body, the person commits an offence and is liable to a maximum fine of $5,000. or maximum imprisonment of 1 year or both.

41. Government social media accounts:

(1) DTO shall regulate the social media accounts of public bodies through standards, guidelines and specifications to be developed in section 65.

(2) A public body is obliged to comply with standards, guidelines and specifications developed under subsection 1 and section 65.

(3) A public body shall not operate a social media account online without a written approval from their SRO and DTO.

(4) To obtain approval, a public body must provide, in the prescribed form, details of the social media accounts, including the purposes for the account and the proposed time period for its use.

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

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

(7) DTO 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.

(8) Before taking action under subsection 10, DTO shall give the public body within twenty four hours to remove or rectify the social media account.

(9) 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 commits an offence and is liable to a maximum fine of $5,000 or a maximum imprisonment of 1 year, or both.

(10) A person who 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 commits an offence and is liable to a maximum fine of $5,000 or a maximum imprisonment of 1 year or both.

(11) For the purposes of administering this section, the Director, by force of this law, is the co-admin of all public bodies' social media accounts.

42. Destruction of digital software or digital platform

A person who, without lawful authority removes, destroys, alters or damages system, software and digital platforms commits an offence and is liable to a maximum fine of $35,000 or a maximum imprisonment of 7 years or both.

43. Moving to Paperless

(1) Director shall develop standards, specifications and guidelines on paper reduction made under section 65, while having regard to the following:

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

PART V
Computer Data

44. Computer data governance across Government

(1) For the purpose of this part, a computer data governance refers to the management and protection of government data so that it is accurate, consistent, trustworthy and used in a responsible and ethical manner.

(2) Computer data governance applies to the whole of the government data-value cycle process of data generation, collection, processing, storage, use and sharing of computer data by public bodies.

(3) DTO must-

(a) build capacity for the implementation of computer data governance measures;
(b) provide oversight on computer data infrastructure, such as data register, APIs, cloud-based solutions and other infrastructure related to computer data governance;
(c) manage computer data architecture, including interoperability, integration, reference data, schematics and data relationship; and
(d) manage data-value cycle described in subsection (2).

45. Classifications of Computer data

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

(a) top-secret data if the unauthorized use, disclosure, alteration or destruction of the data results in a significant level of risk to the government;
(b) confidential data if the unauthorized used, disclosure, alteration, or destruction of the data results in a moderate level of risk to the government; or
(c) open data if the unauthorized use, disclosure, alteration, or destruction of the data may result in little or no risk to the government.

(2) Standards in relation to computer data classification made under section 65 is to prescribe security controls to be applied by public bodies for safeguarding computer data against unauthorized use, disclosure, modification or destruction having regard to the classifications of data referred to in subsection (1).

46. Unlawful use of Top Secret and Confidential Computer Data

(1) Any person who stores, reproduces, alters, modifies, disseminates or uses a top secret data unless authorized by law, commits an offence and is liable to a maximum fine of $50,000 or a maximum imprisonment of 25 years or both

(2) A person who, without lawful authority, accesses, uses, reproduces or disseminates confidential data commits an offence and is liable to a maximum fine of $15,000 or a maximum imprisonment of 3 years or both.

47. Public access to computer data

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

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

(3) A person shall not access any computer data stored by a public body, unless-

(a) the SRO of the public body grants permission;
(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 r.
(c) in the case of personal data of a child under eighteen, parents or legal guardians shall give 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;
(b) the type of computer data that will be accessed;
(c) the time period allowed for the computer data access; and
(d) all other requirements or conditions 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 34.

48. Computer 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 Director, 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) Computer data shall be collected and stored by utilizing any electronic device capable of collecting, processing, and storing data in accordance with the regulation and standards made under this Act.

(4) DTO is responsible for the oversight of computer data storage by public bodies, including when a public body converts any data collected in non-electronic form into electronic form.

49. Ownership of computer data in Government Computer Data Repository

(1) All public bodies must use the Government Computer Data Repository for computer storage provided:

(a) the right of ownership remains with that respective public body to its own computer data when stored in the Government Computer Data Repository.

(2) For the avoidance of doubt, subsection (1) extends to computer 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 computer data repository.

(1) A person who, contravenes subsection (3), commits an offence and is liable to a maximum fine of $10,000 or a maximum imprisonment of 2 years, or both.

50. Systems integration

(1) DTO must develop prescribed standards and specifications for system integration.

(2) All public bodies must comply with these standards and specifications for system integration.

(3) DTO shall establish and maintain a register of APIs used by public bodies.

51. Computer data register

(1) DTO shall establish and maintain a Computer Data Register.

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

52. Computer data sharing

(1) A public body must comply with the prescribed standards and specifications for computer data sharing under section 65.

(2) When sharing computer data, a public body must take the necessary precautions to ensure that the sharing of the data is done in a secure manner without causing data privacy violations or unauthorized access.

(3) For the purpose of facilitating data sharing across the government, all public bodies must use a secure data exchange platform developed by DTO under section 31.

53. Computer data in Outer islands

DTO must take reasonable steps to collaborate with any other public body to deliver digital services in the outer islands with respect to the generation, collection, processing, storing, securing, using, and sharing of computer data.

PART VI
ENFORCEMENT

54. Notices

The Secretary may issue a compliance notice under this part in the prescribed form to any public body upon satisfaction that such body has failed to execute its role required under this Act.

55. Directions

(1) The Secretary may, upon the advice of the Minister after consultation with Cabinet, issue a direction in writing to any public body to comply or cooperate to implement the facilitation of the provisions of this Act.

(2) Any public body who willingly fails to comply with the direction issued in subsection (1) may be reported to Cabinet by the Secretary.

56. Access to systems, investigation, etc.

(1) For the purpose of performing its functions under this Act, the Director may-

(a) direct a public body to give DTO physical or virtual access to a system of the public body;

(b) direct a public body to cease using a private network that is not consistent with this Act, the regulations, standards or specifications;

(c) direct a public body to give DTO access to any source data of any format from the public body;
(d) receive, investigate, respond to and publish complaints relating to digital services provided by a public body;
(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;
(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.

(g) examine any records or documents of a public body relating to ICT project, 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 DTO's functions.

(2) A direction under subsection (1) (a), (b) or (f) must be in writing to SRO.

57. Powers of DTO officers

(1) DTO officer has, in carrying out enforcement actions under this Part, powers to do all or any of the following upon approval from the Director:

(a) enter and search premises or system to ascertain whether non-compliance with this Act has occurred;
(b) interview a person where the officer believes, on reasonable grounds, that he has knowledge or information regarding non-compliance with this Act;
(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.

58. Enforcement Measures

(1) There shall be an enforcement team consisting of-

a) Secretary as Chairperson;
b) Director for DTO;
c) Director of Public Prosecution;
d) Solicitor General;
e) Accountant General;

f) Commissioner of Police; and
g) any other person the Secretary may consider necessary.

(2) The Enforcement team shall;

a) oversee that all sections of this Act are implemented to the best standard expected; and
b) report on the progress of the Act in their respective areas of employment as required under this Act.

3) The report shall include-

a) the effectiveness and efficiency of the Act;
b) the issues for enforcement and implementation; and
c) the plan of the Ministry in overcoming issues.

4) The Secretary as the Chairperson of the Enforcement Team shall;

a) convene the meeting of an Enforcement team twice a year; and
b) provide a report to Cabinet one week after the sitting of the Enforcement team.

5) Failure to provide this report in a timely manner entitles the Secretary to the Cabinet to demand an explanation from the Secretary.

PART VII
OFFENCES

59. Offences

Any person who contravenes any provisions of this Act commits an offence and is liable to a maximum fine of $35,000 or a maximum imprisonment of 7 years or both.

60. Obstructions

Any person who obstructs the Director or any ICT practitioner in the execution of his or her duties under this Act commits an offence and is liable to a maximum fine of $5,000.00 or to a maximum imprisonment of 1 year or both.

61. Matters relating to offences

(1) Prosecution of a person does not prevent proceedings of disciplinary actions against that person or termination of his/her employment under any applicable laws.

(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 person to pay to the Republic the total cost for repairing any damage resulting from the commission of the offence.

(3) In enforcing this Act, DTO may refer any matter of criminal nature to the Kiribati Police Services through Criminal Investigation Division for investigation.

PART VIII
MISCELLANEOUS

62. Immunity

A person engaged in the administrative 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. Absolute Liability

In any prosecution for any offence under this Act, the Prosecution does not need to prove that the offender intended to commit an offence.

64. Regulations

The Minister has the power to make Regulations for the implementation of this Act.

65. Standards, specifications, guidelines, or codes of practice

DTO must develop standards, specifications, guidelines, or codes of practice for the implementation of this Act.

66. Saving and transitional

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 the law.

(1) A public body must, within 3 years of the commencement of this Act, make the necessary arrangements and transmission to comply with the requirements under this Act.

(2) 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 DTO in writing of the details of the account.

(3) 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 1

year of the commencement of this Act, work with DTO to use the government domain as the public body's email domain.

(4) 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 1 year of the commencement of this Act, publish online its website ending in the government domain.

(5) A person conducting ICT business with a public body under a contract or agreement to which this section applies, has 1 year 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.