CYBERSECURITY ACT 2026

Arrangement of Sections

REPUBLIC OF KIRIBATI

(No. 7 of 2026)

I assent

Beretitenti

28/7/2026

AN ACT

entitled

AN ACT TO ESTABLISH THE LEGAL FRAMEWORK FOR NATIONAL CYBERSECURITY, DESIGNATE AND PROTECT CRITICAL INFRASTRUCTURE AGAINST CYBERSECURITY THREATS AND PROVIDE PROCESSES TO ANTICIPATE, PREVENT, MANAGE AND RESPOND TO CYBERSECURITY INCIDENTS AND FOR OTHER CONNECTED PURPOSES;

Commencement date:

_____ 2026

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

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Cybersecurity Act 2026.

2. Commencement

This Act commences on a date that the Minister may by notice appoint.

3. Interpretation

In this Act unless the context otherwise requires:

"**critical infrastructure**" means the physical, electronic or virtual infrastructure assets, networks and information systems designated as such by the Minister under Section 12, and for the purposes of this definition, "virtual infrastructure assets" include any operating system-based or software-based infrastructure assets, whether locally or remotely accessed;

"**cybersecurity**" means the protection of networks and information systems from unauthorised access or attack for the purpose of ensuring their continued availability and integrity, and the integrity and confidentiality of information stored in, processed by or transmitted through them;

"**cybersecurity incident**" means an event that compromise, or has the potential to compromise, the confidentiality, integrity, or availability of an information system or the information processed by that system;

"**Director**" means the director responsible for the DTO appointed under the Digital Government Act 2023;

"**DTO**" means the Digital Transformation Office established in the Digital Government Act 2023;

"**information system**" means a system composed of hardware, software, applications, and networks that processes, stores or transmits data;

"**Minister**" means the Minister responsible for information and communications technology or such other minister designated as responsible for cybersecurity;

"**Ministry**" means the Ministry responsible for information and communications technology or such other ministry designated as responsible for cybersecurity;

"**operator of critical infrastructure**" means any person or entity that owns, operates, manages or controls critical infrastructure or the information systems supporting such infrastructure, and where more than one person or entity performs such functions, each such person or entity shall be considered an operator for the purposes of this Act;

"**person**" means an individual, private entity, public body, state-owned enterprise, agency or any other body;

"**public body**" means the Government's office including Island Councils, Judiciary, the Maneaba ni Maungatabu and statutory bodies but does not include state-owned enterprises;

"**Secretary**" means the Secretary responsible for information and communications technology under the Digital Government Act 2023;

"National CERT" means the national computer emergency response team described in Section 10;

"**Sectoral CERT**" means a sector-specific computer emergency response team established under Section 11;

"Significant cybersecurity incident" means a cybersecurity incident that materially affects, or is likely to materially affect, the confidentiality, integrity, or availability of an information system or the services it supports; and

"**Working Group**" means the Kiribati Cybersecurity Working Group established in Section 9.

4. Administration

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

(2) The Minister shall have the power to delegate in writing the administration of this Act and any other powers or functions assigned under this Act to the Secretary, Director and any other officers within the Ministry as the Minister considers appropriate.

5. Republic to be bound

This Act binds the Republic.

6. Objectives

The objectives of this Act are to:

(a) designate institutions and provide for processes to anticipate, prevent, manage and respond to cybersecurity incidents;

(b) ensure that operators of critical infrastructure adopt cybersecurity measures and practices and collaborate on matters of cybersecurity; and

(c) promote the development and awareness of cybersecurity.

PART II – NATIONAL CYBERSECURITY

7. National Cybersecurity

(1) The DTO shall be responsible for National Cybersecurity and shall have the following functions, duties and powers:

(a) develop, publish, maintain and oversee the implementation of a national strategy for cybersecurity;

(b) make policies for the protection of critical infrastructure, other cybersecurity matters or any other matter relevant to the operation of this Act;

(c) issue and publish cybersecurity standards for the operation of critical infrastructure and guidance on cybersecurity matters, including for the operation of critical infrastructure, assessment of cybersecurity risk and responses to cybersecurity incidents;

(d) provide early warnings, alerts, advisories, announcements and dissemination of information about cybersecurity incidents and threats of such incidents;

(e) maintain a register of critical infrastructure, conduct or require periodic and *ad hoc* audits or inspections of such infrastructure and conduct penetration

testing of critical such infrastructure to identify vulnerabilities and support cyber resilience;

(f) supervise the activities of the National CERT and any Sectoral CERTs;

(g) facilitate information sharing, including among operators of critical infrastructure, to promote effective management of cybersecurity incidents and threats of such incidents;

(h) recommend to law enforcement the prosecution of relevant offences and provide technical digital forensic support on request;

(i) promote awareness of cybersecurity risks, cybersecurity skills and knowledge, cybersecurity practices and research and development of technologies to enhance cybersecurity;

(j) advise ministries, departments and agencies of the Republic of Kiribati on matters of cybersecurity, including on legislation and regulatory measures to further the national strategy for cybersecurity, policies relevant to cybersecurity and this Act;

(k) provide trainings to ministries, departments and agencies of the Republic of Kiribati on cybersecurity matters;

(l) facilitate the Republic of Kiribati's compliance with internationally accepted cybersecurity principles, including any standards and obligations laid down by international agreements and treaties to which the Republic of Kiribati is a party;

(m) represent the Republic of Kiribati in relation to international organisations, foreign governments and private sector organisations on matters of cybersecurity; and

(n) any other functions, powers or duties prescribed in this Act.

8. National Cybersecurity Emergency

(1) Where the Minister determines that a serious cybersecurity threat exists affecting national security or critical infrastructure, the Minister may declare a cybersecurity emergency.

(2) During such emergency, the Minister may direct operators of critical infrastructure to implement specified measures to mitigate the threat.

(3) Any such directions shall be proportionate and limited in duration.

PART III – KIRIBATY CYBERSECURITY WORKING GROUP

9. Kiribati Cybersecurity Working Group

(1) The Kiribati Cybersecurity Working Group is hereby established. The Working Group shall facilitate the development, coordination, and monitoring of cybersecurity activities and programmes.

(2) The members of the Working Group shall be appointed and removed by Secretary, upon the advice of the Director.

(3) Members of the Working Group shall comprise:

(a) the representative of the DTO shall serve as chairperson;

(b) one or more information and communications technology professionals with a technical background, including expertise in information security and cybersecurity;

(c) one or more members representing any such operators of critical infrastructure, or group of such operators;

(d) one or more members representing such ministries, agencies or departments ;

(e) one or more members representing law enforcement; and

(f) any other members representing the interests of academia, NGOs, civil society, or other relevant stakeholders

(4) Represented stakeholders described in subsection (3) may nominate candidate members for consideration by the Secretary for appointment.

(5) The Working Group shall have the following functions and duties:

(a) serve as a forum for the DTO, information and communications technology professionals, operators of critical infrastructure, law enforcement and other stakeholders to share information on matters relating cybersecurity policy;

(b) coordinate and strengthen collaboration among stakeholders on cybersecurity matters;

(c) advise the Director on cybersecurity issues;

(d) provide guidance in the issuance by the DTO of:

(i) cybersecurity standards for the operation of critical infrastructure;

(ii) any early warnings, alerts, advisories, announcements and dissemination of information about cybersecurity incidents and threats of such incidents; and

(iii) cybersecurity measures to be implemented by public or private sector entities or any other matter relevant to the operation of this Act.

(e) prepare and deliver reports upon the advice of the Director, to the Secretary;

(f) establish the form and manner to be used in the performance of their roles and duties under this Act;

(g) provide feedback and suggestions on proposed or current policies, guidance or actions of the Ministry as applicable; and

(h) perform any other functions and duties consistent with this Act as designated by the Director from time to time.

(6) The Working Group shall meet monthly or at other intervals designated by the Secretary.

(7) The Secretary, shall determine the governance and administrative procedures of the Working Group to the extent not addressed in this section.

(8) The DTO shall provide administrative support for the Working Group as needed.

PART IV – COMPUTER EMERGENCY RESPONSE TEAMS

10. The National CERT

(1) The DTO shall maintain and operate the National CERT.

(2) The Director shall be responsible for the oversight, administration and strategic direction to the National CERT.

(3) The National CERT shall have the following duties and functions:

(a) receive and assess reports of cybersecurity incidents and threats of such incidents from operators of critical infrastructure and any others that may report such incidents or threats to it;

(b) develop mechanisms to encourage the voluntary reporting of cybersecurity incidents and threats of such incidents;

(c) provide cybersecurity incident response services to operators of critical infrastructure, government, local businesses and the general public;

(d) maintain points of contact available 24 hours a day, seven days a week to receive reports and requests for services;

(e) assist operators of critical infrastructure, and others on request, in taking preventative, mitigating and remedial measures and coordinating responses in relation to cybersecurity incidents and threats of such incidents;

(f) coordinate activities with those of any Sectoral CERT established under Section 11;

(g) monitor trends in and provide dynamic risk analysis of cybersecurity incidents and threats of such incidents that may affect the Republic of Kiribati;

(h) cooperate with international organisations, foreign governments, private sector organisations and computer security and incident response teams and similar teams of other jurisdictions for the exchange of technical information and the development and implementation of preventative, mitigating and remedial measures in relation to cybersecurity incidents and threats of such incidents; and

(i) conduct defensive cybersecurity operations, including the deployment of technical measures to prevent, detect, and contain malicious cyber activity affecting government systems, critical infrastructure, and other networks within the Republic of Kiribati; and

(j) promote and maintain a secure digital government environment by ensuring that government information systems, applications, and networks are designed, operated, and maintained with appropriate cybersecurity safeguards; and

(k) ensure that government digital infrastructure contains and maintains appropriate security control technologies, including systems for authentication, access control, monitoring, and encryption, consistent with applicable national and international standards; and

(l) promote cyber resilience by developing and implementing measures to ensure that services essential for everyday life in the Republic of Kiribati remain effective and operation during, and recover quickly after, cybersecurity incidents and threats of such incidents; and

(m) monitor for, analyse, and take measures to mitigate cybersecurity threats;

(n) may classify cybersecurity incidents according to their severity, impact or scope;

(o) set out reporting obligations depending on classification of a cybersecurity incident; and

(p) perform such other defensive or operational cybersecurity functions as may be prescribed by this Act, including functions relating to the classification of cybersecurity incidents in accordance with a framework prescribed by regulations, or as may be designated in writing by the Director.

(4) The National CERT shall establish, maintain and update a cybersecurity incident register that records the following information about each cybersecurity incident reported to it:

(a) time and date of the incident;

(b) the nature of the incident and potential impact on the parties and systems affected;

(c) the scope and extent of damage caused to any critical infrastructure; and

(d) any basic forensic information available that may be relevant to an investigation by law enforcement.

11. Sectoral CERTs

(1) The DTO shall periodically consult with relevant ministries, departments and agencies of the Republic of Kiribati, and operators of critical infrastructure to determine whether establishment of one or more Sectoral CERTs is warranted in a particular sector of the economy or society.

(2) In making a determination under subsection (1), the DTO shall consider:

(a) the particular nature and extent of cybersecurity risks facing such sector;

(b) the criticality of such sector;

(c) the preparedness of operators of critical infrastructure in such sector for cybersecurity incidents and threats of such incidents; and

(d) whether establishment of a Sectoral CERT is feasible and would likely improve cybersecurity in such sector.

(3) If the DTO determines that a Sectoral CERT is warranted under subsection (1), the DTO shall direct operators of critical infrastructure in any particular sector of the economy to establish a Sectoral CERT.

(4) Upon establishment of a Sectoral CERT under subsection (3), the DTO shall specify the duties and functions that such Sectoral CERT will have with respect to the relevant sector of the economy.

(5) Unless otherwise determined by the DTO with approval of the Secretary, the cost of a Sectoral CERT established under subsection (3) shall be borne by operators of critical infrastructure of the sector concerned.

(6) Where the sector concerned includes more than one operator of critical infrastructure and such operators do not agree on the allocation among them of the costs of the Sectoral CERT, the DTO shall determine the allocation of such costs among them.

(7) A Sectoral CERT shall report to and be supervised by the DTO and shall keep the minister and any regulatory authority responsible for the relevant sector informed of its activities.

PART V – CRITICAL INFRASTRUCTURE

12. Designation of critical infrastructure

(1) From time to time, the Minister acting on the advice of the Director, shall designate physical, electronic or virtual infrastructure assets, networks or information systems as critical infrastructure if the Minister considers that they are essential for:

(a) national security; or

(b) the economic and social well-being of the population of the Republic of Kiribati.

(2) In making a designation under subsection (1), the Minister shall consider the importance of the relevant physical, electronic or virtual infrastructure assets, networks or information systems to:

(a) the security, defence or international relations of the Republic of Kiribati;

(b) the provision of services relating to:

(i) electronic communications;

(ii) banking and other financial services;

(iii) electric power;

(iv) water and wastewater;

(v) healthcare and public health;

(vi) agriculture and food distribution;

(vii) emergency services;

(viii) fisheries;

(ix) tourism; and

(x) public transportation; and

(c) the legislature, executive and judiciary branches, and law enforcement and security agencies.

(3) The Minister, upon the advice of the Director, shall remove a designation of critical infrastructure if such designation is no longer warranted.

13. Registration of designated critical infrastructure

(1) The DTO shall inform operators of critical infrastructure of a designation made or removed under Section 12.

(2) The DTO shall maintain an up-to-date register of designated critical infrastructure, including a description of the infrastructure, the identity and contact information of each operator of critical infrastructure and any other relevant information required to be included by the DTO.

(3) A registered operator of critical infrastructure shall notify the DTO of any change in ownership of the critical infrastructure or any change in the person or entity responsible for operating such critical infrastructure within 30 days after such change.

(4) The DTO may issue and publish additional procedures for the registration and notification requirements under this section.

14. Required information from operators of critical infrastructure

(1) From time to time, the DTO may, by written notice, require an operator of critical infrastructure to furnish such information to the DTO as it deems necessary to assess the security of the critical infrastructure and cybersecurity measures in place to protect it.

(2) A written notice under subsection (1) shall:

(a) describe the information required;

(b) provide the reasons for requesting such information;

(c) specify the form and manner in which the requested information is to be provided; and

(d) specify the time period within which the information must be provided.

(3) If a material change is made to the design, configuration, security or operation of the critical information infrastructure after any information has been furnished to the DTO pursuant to a notice under subsection (1), the operator of the critical infrastructure shall provide the DTO with a written report summarising the change and any impact on the security of the critical infrastructure not later than thirty days after such change is implemented.

(4) For the purposes of subsection (3), a change is material if it affects or is likely to affect the ability of the operator of critical infrastructure to respond to a cybersecurity incident or threat of such incident affecting the critical infrastructure.

15. Standards and audits

(1) The DTO may, in consultation with appropriate sector regulators and any Sectoral CERTs, issue and publish cybersecurity standards for the operation of critical infrastructure generally, and any specifically applicable to any particular critical infrastructure, that the DTO considers appropriate for the prevention, mitigation or remedy of cybersecurity incidents.

(2) The DTO may, with the assistance of any Sectoral CERT or any other expert organisation, conduct or require periodic or *ad hoc* audits and inspections of critical

infrastructure to ensure compliance with this Act, and any policies, regulatory measures or standards made under it.

(3) The DTO shall make efforts to coordinate any such audit or inspection requirements with any appropriate sector regulators, to the extent such entities are deemed relevant by the DTO.

PART VI – OBLIGATIONS OF OPERATORS OF CRITICAL INFRASTRUCTURE

16. Periodic assessments

(1) An operator of critical infrastructure shall conduct and submit copies of periodic cybersecurity assessments relating to such infrastructure to the DTO.

(2) The DTO may prescribe the form and manner of periodic assessments under subsection (1).

(3) A periodic assessment under subsection (1) shall include an assessment of:

(a) risk and potential consequences of cybersecurity incidents relating to its critical infrastructure;

(b) vulnerability to and preparedness and sufficiency of mitigating measures for cybersecurity incidents;

(c) steps required to ensure readiness for preventing, mitigating and responding to cybersecurity incidents; and

(d) any other matters prescribed by the Director.

17. Appointment of Chief Information Security Officers

An operator of critical infrastructure shall appoint a member of senior management as Chief Information Security Officer or an equivalent role responsible for oversight of:

(a) the operator's cybersecurity preparedness, monitoring and reporting; and

(b) coordination with the DTO and other relevant entities.

18. Obligation to maintain appropriate policies, practices and procedures

(1) An operator of critical infrastructure shall develop, maintain and implement appropriate and proportionate technical and organisational policies, practices and processes to:

(a) manage risks posed to the security of its network and information infrastructure on which its critical infrastructure relies; and

(b) prevent, mitigate and remedy cybersecurity incidents,

with a view to ensuring the continuity of services relying on its critical infrastructure.

(2) An operator of critical infrastructure shall:

(a) communicate to its staff the policies, practices and procedures required by subsection (1) as appropriate to implement them effectively while ensuring their confidentiality;

(b) keep records evidencing its compliance with the requirements of this Part and any other applicable requirements relating to cybersecurity; and

(c) make available to the DTO upon request copies of policies, practices, procedures, and records required by subsection (1).

19. Obligation to manage cybersecurity risks

(1) An operator of critical infrastructure shall establish, implement and maintain a risk management framework for cybersecurity.

(2) The framework shall identify, assess and manage risks to network and information systems supporting critical infrastructure.

(3) The operator shall regularly review and update the framework in accordance with standards prescribed under this Act.

20. Obligation to manage Third-Party and Supply Chain cybersecurity risks

(1) An operator of critical infrastructure shall take reasonable measures to manage cybersecurity risks arising from third-party suppliers, service providers and contractors.

(2) Such measures shall include appropriate contractual, technical and organisational safeguards.

(3) The Minister may prescribe regulations relating to supply chain risk management.

21. Duty to report cybersecurity incidents

(1) An operator of critical infrastructure that is the subject of a cybersecurity incident or threat of one shall:

(a) gather information about the incident or threat, including the nature and impact of the cybersecurity incident;

(b) assess risk to the critical infrastructure, customers, suppliers and other stakeholders;

(c) take appropriate preventative, mitigating and remedial measures to limit such risk;

(d) report all material information about the significant cybersecurity incident to the National CERT and any relevant Sectoral CERT within twenty-four hours after the incident is detected, in a form or manner that may be prescribed by the National CERT or such Sectoral CERT;

(e) provide such other information as the National CERT or any relevant Sectoral CERT may request relating to the cybersecurity incident; and

(f) allow the National CERT and any relevant Sectoral CERT to access its network and information infrastructure for the purpose of:

(i) analysing the cybersecurity incident;

(ii) detecting any other potential threats of such incidents;

(iii) identifying any vulnerabilities in such network and information infrastructure; and

(iv) advising on preventative, mitigating or remedial measures.

22. Obligation to take preventative, mitigating or remedial action

(1) In connection with:

(a) an audit or inspection under Section 15;

(b) an assessment under Section 16;

(c) a reported cybersecurity incident under Section 21; or

(d) otherwise as necessary,

the DTO, any relevant Sectoral CERT, the minister and any regulatory authority responsible for the relevant sector, may order an operator of critical infrastructure to take preventative, mitigating or remedial action in relation to a cybersecurity incident or threat of one.

(2) Any order under subsection (1) shall be reasonable and proportionate taking into account the risk of the cybersecurity incident, and the costs and anticipated effect of the preventative, mitigating or remedial action.

(3) An operator of critical infrastructure shall comply with the order referred to in subsection (1).

23. Operator inability to comply with obligations

An operator of critical infrastructure shall inform the DTO where the operator is unable for financial, legal or technical reasons to comply with the operator's obligations under this Part or Part IV, and the Director may grant exceptions to or modify prescribed standards in appropriate cases.

PART VII – INFORMATION SHARING

24. Information sharing

(1) The DTO, any Sectoral CERTs and operators of critical infrastructure may share information with each other and with the authorities of other jurisdictions if necessary for:

(a) the purposes of this Act or of facilitating the performance of any functions hereunder;

(b) national security purposes; or

(c) purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

(2) Information shared under subsection (1) may not be further shared by the person with which it is shared under that paragraph for any purpose other than a purpose mentioned in that paragraph unless otherwise agreed by the person that shared it.

(3) The DTO may share information with the public about a cybersecurity incident if the Director is of the view that public awareness is necessary to respond effectively to that cybersecurity incident or prevent a future cybersecurity incident.

(4) Information shared under subsections (1) and (3) shall be limited to information that is relevant and proportionate to the purpose of the information sharing, with due regard to the protection of confidential information and information that may prejudice national security or the legitimate commercial interests of operators of infrastructure.

(5) A person or entity that in good faith, share information with the DTO, a Sectoral CERT, or the National CERT concerning a cybersecurity incident, cyber threat, or vulnerability for the purposes of this Act shall not incur civil or criminal liability for the disclosure of that information.

(6) Information shared under this section shall not be used in civil or administrative proceedings against the person or entity that provided the information unless it is shown that the information was provided in bad faith or with intent to mislead.

(7) The DTO and any Sectoral CERT receiving information under this section shall take reasonable measures to protect the confidentiality of the information and shall ensure that any further disclosure is limited to what is necessary for the purposes specified in subsection (1).

PART VIII – ENFORCEMENT

25. Failure to comply with an obligation

(1) An operator of critical infrastructure that fails to carry out its obligations under Parts IV or V in the absence of an exemption or modification from the DTO under Section 23 commits an offence.

(2) A person who commits an offence under subsection (1) shall, on summary conviction, be liable to a fine not exceeding $100,000 for a first offence or $200,000 for a subsequent offence, and in the case of a continuing offence, to a further fine not exceeding $200 for each day during which the offence continues.

26. Damage to critical infrastructure

A person who, without lawful authority, removes, destroys, alters or damages critical infrastructure commits an offence and is liable to a fine not exceeding $200,000 or a maximum imprisonment of 7 years or both.

27. Offences by persons that are not individuals

(1) A person that is not an individual shall be deemed to commit an offence under this Act if an individual who has a leading position within such person takes action resulting in the commission of such offence:

(a) as a representative of such person;

(b) carrying out duties of such responsibility that such person's conduct may fairly be assumed to represent the policies of such person; or

(c) with authority to exercise control within such person.

(2) A person that is not an individual shall be deemed to commit an offence under this Act where the offence was made possible due to the lack of supervision or control of an individual referred to in subsection (1)(a), (1)(b) or (1)(c).

(3) If a person that is not an individual is deemed to commit an offence under subsections (1) or (2), the relevant individual in such subsections:

(a) may be charged jointly or severally in the same proceedings with the person; and

(b) if the person is found guilty of the offence, shall also be deemed to be guilty of that offence, unless, having regard to the nature of the individual's function in that capacity and to all circumstances, the individual proves:

(i) that the offence was committed without the person's knowledge, consent or connivance; or

(ii) that the individual had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

(4) Any person that is not an individual who commits an offence under this section shall be dealt with under the preceding sections 25 and 26 where applicable.

PART IX – MISCELLANEOUS

28. Power to issue regulations

(1) The Minister shall have the power to issue regulations for the implementation of this Act.

(2) Without prejudice to the generality of subsection (1), the regulations may provide for:

(a) the governance, funding and financial management of the affairs of the DTO;

(b) the manner in which the Secretary or Director may exercise any power or perform any duty or function under this Act; or

(c) any matter that the Minister considers necessary or expedient to give effect to the objectives of this Act.

29. Consequential Amendments

(1) In section 4 of the Digital Government Act 2023, the following definitions shall be repealed:

(a) critical digital infrastructure; and

(b) national computer emergency response team "CERT".

(2) The entirety of division 4 of part II and sections 22, 23 and 28 of the Digital Government Act 2023 shall be repealed.

CYBERSECURITY ACT 2026

EXPLANATORY MEMORANDUM

BACKGROUND

The Cybersecurity Act 2026 provides a legislative framework that designates institutional responsibility for processes to anticipate, prevent, manage and respond to cybersecurity incidents. It also ensures that operators of critical infrastructure adopt cybersecurity measures and practices and collaborate on matters of cybersecurity and promotes the development and awareness of cybersecurity.

This Act consists of nine Parts and twenty-six sections, which are explained in detail below.

PART I – PRELIMINARY

Part I specifies the name of the Act as the Cybersecurity Act 2025 and that it commences on a date to be appointed by the Minister. It also sets out a list of defined terms that are used in the Act.

This part also names the Minister as responsible for the administration of the Act and specifies that the Act binds the Republic. It sets out the objectives of the Act, which include designating institutions and providing for processes to anticipate, prevent, manage and respond to cybersecurity incidents, ensuring that operators of critical infrastructure adopt cybersecurity measures and practices and collaborate on matters of cybersecurity and promoting the development and awareness of cybersecurity.

PART II – NATIONAL CYBERSECURITY

Part II outlines the role of the Digital Transformation Office (DTO) as the lead agency responsible for national cybersecurity in Kiribati. It empowers the DTO to develop and implement a national cybersecurity strategy, establish policies and standards for the protection of critical infrastructure, and coordinate national efforts to prevent, detect, and respond to cybersecurity threats and incidents.

It also authorizes the DTO to provide early warnings and advisories, supervise the activities of the national and sectoral Computer Emergency Response Teams (CERTs), facilitate information sharing, promote cybersecurity awareness and capacity building, and represent Kiribati in international cybersecurity matters.

PART III – KIRIBATI CYBERSECURITY WORKING GROUP

Part III establishes the Kiribati Cybersecurity Working Group to support the development, coordination, and monitoring of national cybersecurity activities and programmes. The Working Group serves as a multi-stakeholder forum bringing together representatives from DTO), operators of critical infrastructure, law enforcement, ICT professionals, government agencies, academia, and civil society to enhance collaboration on cybersecurity matters.

It outlines the composition, appointment process, and functions of the Working Group, which include providing advice and guidance to the DTO on cybersecurity standards, policies, and incident response measures, as well as preparing reports for the Secretary. The Part also authorises the Secretary to determine the governance and administrative procedures of the Working Group and mandates the DTO to provide administrative support.

PART IV – COMPUTER EMERGENCY RESPONSE TEAMS

Part IV requires the DTO to maintain and operate the CERT. It sets out the duties and functions of the CERT, which include receiving and assessing reports of cybersecurity incidents, providing incident response services, assisting in preventive and remedial measures, maintaining 24/7 contact points, and coordinating responses to cyber threats. The CERT is also mandated to cooperate with international partners, conduct defensive cybersecurity operations, and promote cyber resilience across government systems, critical infrastructure, and other networks.

This part also authorises the DTO, in consultation with relevant ministries, departments, agencies, and operators of critical infrastructure, to determine whether establishment of one or more Sectoral CERTs is warranted in a particular sector of the economy or society and to direct the establishment of a Sectoral CERT by such operators of critical infrastructure. Costs of the Sectoral CERT are to be borne by the operators of critical infrastructure.

PART V – CRITICAL INFRASTRUCTURE

Part V empowers the Minister, on the advice of the Director, to designate or remove physical, electronic, or virtual infrastructure assets, networks, or information systems as critical infrastructure if the Minister considers that they are essential for national security the economic and social well-being of the population of the Republic of Kiribati. It also sets out factors the Minister may consider when considering such a designation.

This part also authorises the DTO to maintain an up-to-date register of designated critical infrastructure and to notify operators of any designation or removal. It also mandates the DTO to request information from operators to assess their cybersecurity measures and to require reports of any material changes affecting the security of their infrastructure. The DTO is further required to issue cybersecurity standards and conduct audits or inspections, in coordination with sector regulators and Sectoral CERTs, to ensure compliance and strengthen the protection and resilience of critical infrastructure.

PART VI – OBLIGATIONS OF OPERATORS OF CRITICAL INFRASTRUCTURE

Part VI requires operators of critical infrastructure to conduct and submit to the DTO copies of periodic cybersecurity assessments, appoint a Chief Information Security Officer and develop, maintain and implement appropriate and proportionate technical and organisational policies, practices. It also imposes an obligation on operators of critical infrastructure to report cybersecurity incidents to the National CERT and any relevant Sectoral CERT and authorizes the DTO to order an operator of critical infrastructure to take preventative, mitigating or remedial action in relation to a cybersecurity incident or threat of one. Where operators are unable to meet these obligations for financial, legal, or technical reasons, the Director may grant exceptions or modify prescribed standards.

PART VII – INFORMATION SHARING

Part VII authorises the DTO, any Sectoral CERTs and operators of critical infrastructure to share information with each other and with the authorities of other jurisdictions as necessary for certain cybersecurity purposes.

PART VIII – ENFORCEMENT

Part VIII makes it an offence for an operator of critical infrastructure to fail to carry out its obligations under Parts IV or V in the absence of an exemption or modification from the DTO, subject to a fine not exceeding $10,000 for a first offence or $20,000 for a subsequent offence, and in the case of a continuing offence, to a further fine not exceeding $100 for each day during which the offence continues.

This part also makes it an offence for any person to, without lawful authority, remove, destroy, alter or damage critical infrastructure, subject to a maximum fine of $35,000 or a maximum imprisonment of 7 years or both.

This part clarifies that liability for such offences by persons who are not individuals may be incurred by actions taken by individuals with leading positions within such person. Such individuals may in certain circumstances also be jointly or severally charged for such offences.

PART IX – MISCELLANEOUS

Part IX grants the Minister the power to make regulations for the implementation of the Act.

This part also states consequential amendments repeal the definitions of "critical digital infrastructure" and "national computer emergency response team (CERT)," the entirety of division 4 of part II and sections 22, 23 and 28 of the Digital Government Act 2023.

HON. ALEXANDER TEABO

Minister for Information, Communication and Transport

LEGAL REPORT

I hereby certify that in my opinion none of the provisions of the above Act are in conflict with the Constitution and that the Beretitenti may properly assent to the Act.

MS. PAULINE BEIATAU

TE TIA KAETI TUA

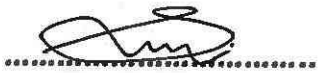
CERTIFICATE OF THE CLERK OF THE MANEABA NI MAUNGATABU

This printed impression of the Cybersecurity Act 2026 has been carefully examined by me with the Bill which passed the Maneaba ni Maungatabu on the 23rd April 2026 and is found by me to be a true and correctly printed copy of the said Bill.

Eni Tekanene

Clerk of the Maneaba ni Maungatabu

Published by exhibition at the Maneaba ni Maungatabu this ..... day of ..... 2026.



Eni Tekanene

Clerk of the Maneaba ni Maungatabu