CYBERSECURITY ACT, 2025

No. 21 **of 2025**

ARRANGEMENT OF SECTIONS

SECTION

PART I — *Preliminary*

1. Short title and commencement
2. Interpretation
3. Application of Act
4. Relationship with other Acts

PART II — *National Cybersecurity Authority*

5. Establishment of National Cybersecurity Authority
6. Objectives of Authority
7. Regulatory functions of Authority
8. Administrative functions of Authority
9. Seal of Authority
10. Establishment of Cybersecurity Multisectoral Committee
11. Functions of Committee

PART III — *Board of the Authority*

12. Establishment of Board
13. Membership of Board
14. Directions by Minister
15. Tenure of office
16. Disqualification, removal and resignation of members
17. Vacation of office
18. Filling of vacancies
19. Remuneration and allowances

PART IV — *Meetings and proceedings of Board*

20. Meetings of Board
21. Appointment of Chairperson and election of Vice-Chairperson
22. Quorum and procedure at meetings
23. Disclosure of interest

24. Confidentiality
25. Committees of Board
26. Co-opted members

PART V — *Chief Executive Officer and staff of the Authority*

27. Chief Executive Officer
28. Secretary to Board
29. Appointment of senior and other staff

PART VI — *Financial Provisions*

30. Funds of Authority
31. Strategic and annual plan
32. Financial year
33. Accounts and audit
34. Pension and other funds
35. Annual report

PART VII — *Licensing of Cybersecurity Service Providers*

36. Licensable cybersecurity services
37. Licensing of cybersecurity service providers
38. Grant of licence
39. Renewal of licence
40. Assessment of application for licence
41. Variation of license
42. Non-transferability of licence
43. Suspension of licence
44. Revocation of license

PART VIII — *Critical Information and Critical National Information Infrastructure*

45. Designation of critical information and critical national information infrastructure
46. Categories of critical information and critical national information infrastructure
47. Registration of critical information and critical national information infrastructure
48. Withdrawal of designation of critical information and critical national information infrastructure
49. Hosting of critical information and critical national information infrastructure
50. Change in ownership of critical information and critical national information infrastructure

51. Auditing of critical information and critical national information infrastructure
52. Non-compliance to audit requirements
53. Duty to report cybersecurity incidents in respect of critical information and critical national information infrastructure

PART IX — *Botswana Computer Security Incident Response Team*

54. Establishment of Botswana Computer Security Incident Response Team
55. Sectoral cyber incident response teams
56. Duty to report cybersecurity incident
57. Cybersecurity incident monitoring and response system
58. Early warning system

PART X — *International Cooperation*

59. International cooperation

PART XI — *Miscellaneous Provisions*

60. Registers
61. Request for information
62. Exemption from liability of officers of Authority and members of Board
63. Review of decisions of Authority
64. Codes of practice and standards
65. Exemptions
66. Regulations

An Act to provide for the establishment of structures to promote cybersecurity and capacity building in Botswana; to regulate and promote the development of cybersecurity activities in the country; to provide for the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide for secure and cyber resilient systems for the protection of users; to provide for the governance and securing of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the basis for the prevention and resolution of cyber incidents; and for matters connected or incidental therewith.

Date of Assent: 05.11.2025
Date of Commencement: ON NOTICE
ENACTED by the Parliament of Botswana.

PART I — *Preliminary*

Short title and commencement

1. This Act may be cited as the Cybersecurity Act, 2025, and shall come into operation on such date as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

2. In this Act, unless the context otherwise requires —

"Authority" means the National Cybersecurity Authority established under section 5;

"Board" means the Board of the Authority established under section 12;

"Chief Executive Officer" means the Chief Executive Officer of the Authority, appointed under section 27;

"computer or computer system" means an electronic, magnetic or optical device or a group of interconnected or related devices, including the Internet, one of more or which, pursuant to a programme, performs the automatic processing of data;

"critical information" means computer data that relates to public safety, public health, economic stability, national security, international stability and the sustainability and restoration of critical cyberspace, including —

(*a*) personal data that is managed, stored or transmitted through critical national information infrastructure or processed by an owner;

(*b*) information relating to any research and development in relation to critical national information infrastructure;

(*c*) information needed to operate critical national information infrastructure; and

(*d*) information relating to risk management and business continuity in relation to critical national information infrastructure;

"critical national information infrastructure" means information and communication infrastructures, whether physical or virtual, which are essential for the maintenance of vital societal functions, including —

(*a*) public health and safety;

(*b*) national security;

(*c*) economic stability; and

(*d*) the social well-being of people, the incapacity, disruption or destruction of which would significantly —

(i) cause the interruption of life sustaining services, including but not limited to the supply of water, health services and energy,

(ii) have a debilitating effect on the economy,

(iii) result in massive casualties or fatalities, or

(iv) cause failure or substantial disruption of the money market;

"critical sector" means the services critical to the functioning of the nation's security, public order, health, economy and safety, including —

(*a*) telecommunications and IT systems;

(*b*) transport;

(*c*) energy;

(*d*) water;

(*e*) financial sector;

(*f*) healthcare; and

(*g*) public and e-government services;

"cyber resilience" means the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources;

"cybersecurity" means the ability of internet-connected computers or computer systems or electronic systems or information systems through —

(*a*) tools;

(*b*) policies;

(*c*) security concepts;

(*d*) security safeguards, guidelines, risk management approaches, actions, training and technologies,

to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those computers, information or computer systems;

"cybersecurity service" means a service provided by a person or entity, that is intended primarily for or aimed at ensuring the cybersecurity of or safeguarding of a computer, computer system or information system belonging to another person or entity, and includes —

(*a*) assessing, testing or evaluating the cybersecurity of a computer, computer system or information system by searching for vulnerabilities that may compromise the cybersecurity defences of the computer or computer system or information system;

(*b*) conducting a forensic examination of a computer, computer system or information system;

(*c*) investigating and responding to a cybersecurity incident that has affected a computer, computer system or information system by conducting assessments of the computer, computer system or information system —

(i) to identify and remove elements relating to the cyber incident,

(ii) to identify the root cause of the cybersecurity incident, and

(iii) which involve circumventing the controls implemented in the computer, computer system or information system;

(*d*) conducting a thorough examination of a computer, computer system or information system to detect any cybersecurity threat or incident that may have already penetrated the cybersecurity defences of the computer, computer system or information system, and that may have evaded detection by conventional cybersecurity solutions;

(*e*) designing, selling, importing, exporting, installing, maintaining, repairing or servicing of one or more cybersecurity solutions;

(*f*) monitoring of the cybersecurity of a computer, computer system or information system by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer, computer system or information system for the purpose of identifying cybersecurity threats to the computer, computer system or information system;

(*g*) maintain control of the cybersecurity of a computer, computer system or information system by effecting management, operational and technical controls, for the purpose of protecting the computer, computer system or information system against any unauthorised effort to adversely affect its cybersecurity;

(*h*) assessing or monitoring the compliance of a cybersecurity service provider with the service provider's cybersecurity policy;

(*i*) providing advice in relation to cybersecurity solutions, including —

(i) advice on a cybersecurity program, and

(ii) identifying and analysing cybersecurity threats and providing advice on solutions or management strategies to minimise the risk posed by cybersecurity threats;

(*j*) providing advice in relation to any practices that can enhance cybersecurity; and

(*k*) providing training or instruction in relation to any cybersecurity service, including the assessment of the training, instruction or competencies of another person in relation to any such activity;

"cybersecurity service provider" means a person licensed under the Act to provide a cybersecurity service;

"data" means –

(*a*) any representation of facts, information or concepts in a form suitable for processing in a computer, computer system or information system;

(*b*) any information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; or

(*c*) any programme suitable to cause a computer, computer system or information system to perform a function, and includes traffic data and subscriber information;

"device" includes —

(*a*) a computer programme, code, software or application;

(*b*) a component of a computer or computer system, such as a graphic card, memory card, chip or processor;

(*c*) physical or virtual hardware or equipment that provides one or more computing functions;

(*d*) a computer data storage medium; or

(*e*) any input or output device;

"digital product" means a software, application or content distributed electronically, including —

(*a*) mobile and desktop applications;

(*b*) operating systems;

(*c*) firmware;

(*d*) digital games;

(*e*) e-books;

(*f*) audio visual media; or

(*g*) embedded software in connected devices;

"digital services" means any service that is delivered or accessed through electronic technology and internet-based platforms;

"digital technology" means any electronic tool, system, device, resource or infrastructure that generates, stores, processes or transmits data, including —

(*a*) cloud computing;

(*b*) artificial intelligence;

(*c*) blockchain;

(*d*) robotics; and

(*e*) Internet of Things (IoT);

"electronic communication" means the emission, transmission or reception of information, including voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetic, radio or other electronic waves, optical, electromagnetic system or any agency whether with or without the aid of tangible conduct;

"hosting" means the service of storage of data or providing storage of computing resources for one self or others;

"information system" means a system for generating, sending, receiving, storing or otherwise processing electronic communications;

"law enforcement agency" means —

(*a*) the Botswana Police Service;

(*b*) the Botswana Prisons Service;

(*c*) the Directorate of Corruption and Economic Crime;
(*d*) the Drug Enforcement Agency;
(*e*) the Directorate of Intelligence Service;
(*f*) the Botswana Defence Force;
(*g*) the Chemical, Biological, Nuclear and Radiological Weapons Management Authority; and
(*h*) any other agency that the Minister may by Order published in the *Gazette*, designate for purposes of this Act;

"register" means a catalogue or database of cybersecurity threats and regulatory documents which is kept and maintained by the Authority in terms of section 60; and

"risk" means any reasonably identifiable circumstance or event, having a potential adverse effect on the security of network and information systems.

Application of Act

3. (1) This Act applies to the governance and securing of network and information systems essential for the functioning of the society, including the liability, supervision and the basis for the prevention and resolution of cyber incidents.

(2) This Act shall not apply to the processing of classified information held by the —

(*a*) Botswana Police Service;
(*b*) Botswana Prisons Service;
(*c*) Botswana Defence Force;
(*d*) Directorate of Corruption and Economic Crime;
(*e*) Directorate of Intelligence and Security;
(*f*) Drug Enforcement Agency;
(*g*) Chemical, Biological, Nuclear and Radiological Weapons Management Authority; and
(*h*) Botswana Unfied Revenue Service.

(3) For the purposes of this section, "classified information" means information of such a sensitive nature and value that the unauthorised publication or disclosure thereof would lead to a security risk being posed to the State.

Relationship with other Acts

Cap. 43:14

4. In the event of a conflict or inconsistency between the provisions of this Act and any other law on cybersecurity, the provisions of this Act shall take precedence, except where such conflict or inconsistency is with the provisions of the Data Protection Act.

PART II — *National Cybersecurity Authority*

Establishment of National Cybersecurity Authority

5. (1) There is hereby established a body to be known as the National Cybersecurity Authority.

(2) The Authority shall be a body corporate with a common seal, capable of suing and being sued in its own name and, subject to the provisions of this Act, of doing or performing all such acts or things as bodies corporate may, by law, do or perform.

Objectives of Authority

6. The objectives of the Authority shall be to regulate and promote cybersecurity and cyber resilience, ensuring the effective application of and compliance with this Act.

Regulatory functions of Authority

7. The regulatory functions of the Authority shall be to —

(*a*) establish codes of practice, policies and standards for cybersecurity and the provision of cybersecurity services, and monitor compliance with the codes of practice and standards by the public and private sector owners of critical information and critical national information infrastructure;

(*b*) process applications for and grant licences, permits, permissions, concessions and authorities for services regulated under this Act in such manner, as may be prescribed;

(*c*) approve software products prior to their being placed in the market;

(*d*) provide training and certification of cybersecurity service providers;

(*e*) develop and implement a National Cybersecurity Strategy, including programmes, policies and other cybersecurity initiatives;

(*f*) oversee the functions of any institution established for the purposes of ensuring and promoting cybersecurity;

(*g*) ensure safe, secure, efficient and affordable cybersecurity services and products throughout Botswana;

(*h*) identify, designate and regulate critical information and critical national information infrastructure owners with regards to the cybersecurity of the critical information and critical national information infrastructure;

(*i*) monitor the performance of the regulated cybersecurity sector and licensed cybersecurity service providers;

(*j*) establish and maintain a cybersecurity risk register of –

(i) identified and potential risks,

(ii) the levels and impact of risks, and

(iii) persons licensed to carry out cybersecurity activities; and

(*k*) take such other steps and to perform such other acts as may be required for the achievement of its objects and the proper performance of its functions and duties in terms of the Act.

Administrative functions of Authority

8. The Authority shall —

(*a*) require internal periodic assessment of cybersecurity service providers;

(*b*) prepare and submit periodic reports concerning the state of national cybersecurity for submission to the Minister;

(*c*) conduct a national cyber risk assessment of the activities of critical national information infrastructure owners;

(*d*) advise on national policies in respect of cybersecurity, including cyber resilience and ways of reducing cybersecurity risks; and

(*e*) perform such other administrative functions and duties as may be conferred on the Authority under this Act.

Seal of Authority

9. (1) The seal of the Authority shall be such device as may be determined by the Authority and shall be kept by the Secretary of the Board.

(2) The seal of the Authority shall be authenticated by the signature of the Chief Executive Officer and the Secretary.

(3) In the absence of the Chief Executive Officer, the person performing the functions of the Chief Executive Officer may authenticate the seal in his or her place and, in the absence of the Secretary, the person performing the functions of the Secretary may authenticate in his or her place.

(4) The Chief Executive Officer may, in writing, delegate to another employee of the Authority his or her power to authenticate the seal.

(5) The Secretary may, in writing and with the approval of the Chief Executive Officer, delegate to another officer of the Authority his or her power to authenticate the seal.

(6) A document issued by the Authority and sealed with the seal of the Authority, which seal is authenticated in the manner provided by this section, shall be received and taken to be a true instrument without further proof, unless the contrary is shown.

Establishment of Cybersecurity Multisectoral Committee

10. (1) There is hereby established a Cybersecurity Multisectoral Committee.

(2) The Committee shall consist of nine members appointed by the Authority and, in appointing members of the Committee, the Authority shall ensure that there shall be an equitable distribution of membership as follows —

(*a*) two representatives from the public service;

(*b*) two owners of the critical national information infrastructure;

(*c*) a representative, who shall be a licensed cybersecurity service provider;

(*d*) a representative from the civil society;

(*e*) a representative from the academia;

(*f*) one representative from the cybersecurity profession; and

(*g*) one representative from a law enforcement agency.

(3) Subject to the provisions of this Act, the Committee will regulate its own procedure.

(4) A member of the Committee shall hold office for such period, not exceeding three years, as may be specified in the instrument appointing him or her.

(5) A member whose office expires shall be eligible for re-appointment for one more term, not exceeding three years.

(6) The Authority shall pay such remuneration and expenses as the Authority shall determine, to members of the Committee.

Functions of Committee

11. The functions of the Committee shall be to —

(*a*) assess the effectiveness of policies and measures to combat cybersecurity threats and incidents;

(*b*) make recommendations to the Minister and Authority for legislative, administrative and policy reforms in respect of matters of cybersecurity; and

(*c*) coordinate the national risk assessment to identify, assess and mitigate the risk of cybersecurity threats and incidents emerging from development of new products and new business practices in the cyber space, including the use of new or emerging technologies.

PART III — *Board of the Authority*

Establishment of Board

12. There is hereby established a Board of the Authority, which shall be the governing body of the Authority and shall be responsible for the direction of the affairs and operations of the Authority.

Membership of Board

13. (1) The Board shall consist of 11 members appointed by the Minister, and the members shall be appointed from amongst persons with expertise in —

(*a*) information and communication technology;
(*b*) cybersecurity;
(*c*) information and technology policy or regulation;
(*d*) law;
(*e*) economics;
(*f*) business;
(*g*) engineering;
(*h*) financial accounting;
(*i*) financial intelligence;
(*j*) public policy; and
(*k*) human resource management.

(2) The Board shall be responsible for the general control of the performance and management of the affairs of the Authority, and without derogating from the generality of this provision, the Board shall —

(*a*) determine the general performance of the Authority;
(*b*) determine corporate policy and provide strategic direction for giving effect to the objects and purposes of the Act;
(*c*) establish, implement, assess and improve management systems that are aligned with the goals of the Authority;
(*d*) determine and recommend to the Authority, any fees necessary for any licensed activity to be carried out under this Act;
(*e*) ensure compliance with international instruments or agreements relating to cybersecurity, to which Botswana is a party to; and
(*f*) do such other things as are provided by this Act or as may be necessary for the proper implementation of this Act.

(4) The Chief Executive Officer shall be an *ex-officio* member of the Board.

Directions by Minister

14. (1) The Minister may give to the Board written directions, of a general or specific nature, regarding the exercise of its powers, which directions shall not be inconsistent with this Act or with contractual or other legal obligations of the Board.

(2) The Board shall give effect to the Minister's directions given in accordance with subsection (1).

Tenure of office

15. (1) A member shall hold office for such period, not exceeding five years, as may be specified in the instrument appointing him or her.

(2) A member whose office expires shall be eligible for re-appointment for one more term, not exceeding five years.

Disqualification, removal and resignation of members

16. (1) A person shall not qualify for appointment as a member or continue to hold office as a member where he or she –

(*a*) is at the time of appointment, a member of the National Assembly, a councillor or a member of *Ntlo ya Dikgosi*;

(*b*) has, in terms of a law in force in any country —

(i) been adjudged or otherwise declared bankrupt and has not been discharged,

(ii) made an assignment to, arrangement or composition with his or her creditors, which has not been rescinded or set side;

(*c*) has, within the period of 10 years immediately preceding the date of his or her appointment, been convicted —

(i) of a criminal offence, within Botswana,

(ii) outside Botswana, of an offence which if committed in Botswana, would have been a criminal offence,

and sentenced by a court of competent jurisdiction to imprisonment for six months or more without the option of a fine, whether that sentence has been suspended or not, and for which he or she has not received a free pardon;

(*d*) has, within a period of 10 years immediately preceding the date of his or her appointment, been disqualified or suspended by a competent authority from practising a profession on grounds of misconduct or negligence; or

(*e*) is a holder of a licence or has an interest in a licence issued under this Act.

(2) The Minister may, in writing, suspend from office, a member against whom criminal proceedings are instituted for an offence in respect of which a sentence of imprisonment without the option of a fine may be imposed, and whilst that member is so suspended, he or she shall not carry out any duties under this Act nor be entitled to any remuneration or allowances as a member of the Board.

(3) The Minister shall remove a member from office, if the member —

(*a*) has become subject to a disqualification under subsection (1);

(*b*) is absent without reasonable cause from three consecutive meetings of the Board of which he or she has had notice;

(*c*) has been found to be physically or mentally incapable of performing his or her duties efficiently, and a medical doctor has issued a certificate to that effect;

(*d*) contravenes the provisions of this Act or otherwise misconducts himself or herself to the detriment of the objectives of the Board;

(*e*) has failed to comply with the provisions of sections 23 and 24; or

(*f*) has been convicted of an offence under this Act, or under any other Act for which he or she is sentenced to imprisonment for a term of six months or more without an option of a fine.

(2) For purposes of subsection (1) (*d*), "misconduct" includes any act, done by a member without reasonable excuse, which —

(*a*) amounts to failure to perform in a proper manner, any duty imposed on him or her as such;

(*b*) is prejudicial to the efficient carrying out of the functions of the Authority; or

(c) tends to bring the Authority into disrepute.

(3) A member may resign from the Board by giving 30 days' notice, in writing, to the Minister.

Vacation of office

17. A member shall vacate his or her office and his or her office shall become vacant —

(*a*) if he or she becomes disqualified in terms of section 16 to hold office as a member of the Board;

(*b*) upon his or her death;

(*c*) upon the expiry of such time as the Minister may specify, in writing, notifying the member of his or her removal from office by the Minister;

(*d*) upon the expiry of one month's notice, in writing, to the Chairperson, of his or her intention to resign from office; or

(*e*) if he or she is summarily dismissed by the Minister on the grounds of contravening the provisions of this Act.

Filling of vacancies

18. (1) Where the office of a member becomes vacant before the expiry of the member's term of office, the Minister shall appoint another person to be a member in place of the member who vacates office, until the expiry of a period during which such member would have otherwise continued in office.

(2) Subsection (1) shall not apply where the remainder of the period for which the member whose office has been vacated would otherwise have held office is less than six months.

Remuneration and allowances

19. A member shall be paid such remuneration, travelling expenses and other expenses and allowances, incurred in connection with his or her services on the Board, if any, as the Minister may determine.

PART IV — *Meetings and Proceedings of Board*

Meetings of Board

20. (1) Subject to the provisions of this Act, the Board shall regulate its own proceedings.

(2) The Board shall hold its first meeting on such date and at such place as the Minister may fix and thereafter the Board shall meet at least once in every three months.

(3) Upon giving notice, in writing, of not less than 14 days, a meeting of the Board may be called by the Chairperson, but if the urgency of any particular matter does not permit the giving of such notice, a special meeting may be called upon the giving of a shorter notice.

(4) The notice referred to under subsection (3) shall state —

(*a*) the place and time for the meeting; and

(*b*) the agenda for the meeting.

(5) There shall preside at any meeting of the Board —

(*a*) the Chairperson; or

(*b*) in the absence of the Chairperson, the Vice-Chairperson.

Appointment of Chairperson and election of Vice-Chairperson

21. (1) The Minister shall appoint the Chairperson of the Board from amongst the members appointed under subsection (1).

(2) The members shall, at the first meeting of the Board, elect from amongst their number, the Vice-Chairperson of the Board.

(3) The Chairperson and Vice-Chairperson shall hold office for a period of not more than three years.

(4) On the expiry of the terms of office of the Chairperson or the Vice-Chairperson, or where the Chairperson or the Vice-Chairperson vacates office, a new Chairperson shall be appointed by the Minister and a new Vice-Chairperson shall be elected by the members from among their number at the next meeting of the Board or as soon thereafter as may be convenient.

(5) The Chairperson or Vice-Chairperson may vacate his or her office as such even though he or she remains a member.

(6) The Vice-Chairperson shall exercise the functions of the Chairperson during the period that the Chairperson is absent or unable to act as Chairperson.

Quorum and proceedings at meetings

22. (1) The quorum at any meeting of the Board shall be a simple majority of the members.

(2) A decision of the Board on any question shall be by the majority of the members present and voting at the meeting and, in the event of an equality of votes, the member presiding shall have a casting vote in addition to that member's deliberative vote.

(3) A decision of the Board shall not be rendered invalid by reason of a vacancy on the Board or the fact that a person who was not entitled to sit as a member did so sit.

(4) The Board may invite any person whose presence it deems necessary, to attend and participate in the deliberations of a meeting of the Board, but such person shall have no vote.

Disclosure of interest

23. (1) If a member is present at a meeting of the Board or any committee of the Board at which any matter —

(*a*) in which, an immediate member of his or her family is directly or indirectly interested in a private capacity; or

(*b*) in which the member is directly or indirectly interested in a private capacity,

is the subject of consideration, the member shall, as soon as practicable after the commencement of the meeting, disclose such interest and shall not take part in any consideration or discussion of, or vote on any question touching on the matter.

(2) A disclosure of interest made under subsection (1) shall be recorded in the minutes of the meeting at which it is made.

(3) Where a member fails to disclose his or her interest in accordance with subsection (1) and a decision by the Board is made benefitting such member, or immediate family member of the member, such decision shall be null and void to the extent that it benefits such member or his or her immediate family member.

(4) For the purposes of this section, "immediate family member" means a spouse, son, daughter, sibling or parent.

(5) A member who fails to comply with the provisions of subsection (1) commits an offence and is liable to a fine not exceeding P30 000, or to imprisonment for a term not exceeding six months, or to both.

Confidentiality

24. (1) A member and any other person assisting the Board shall observe and preserve the confidentiality of all matters coming before the Board, and such confidentiality shall subsist even after the termination of their terms of office or their mandates.

(2) Any member or any person to whom confidential information is revealed through working with the Board shall not disclose that information to any other person unless he or she is required to do so in terms of any written law or for purposes of any judicial proceedings.

(3) Any member or any other person who contravenes the provisions of this section commits an offence and is liable to a fine not exceeding P50 000, or to imprisonment for a term not exceeding six months, or to both.

Committees of Board

25. (1) The Board may, for the purpose of performing the functions of the Authority, establish such committees as it considers appropriate, and may delegate to any committee, such functions as it considers necessary.

(2) The Board may appoint to the committees constituted under subsection (1), such number of persons, from amongst the members, as it considers appropriate, to be members of such committees and such persons shall hold office for such period as the Board shall determine.

(3) Subject to any direction given by the Board, a committee may regulate its own procedure.

(4) The meetings of a committee shall be held at such times and places as the committee may determine, or as the Board may direct.

(5) The chairperson of each committee, appointed by the Board from amongst its members, shall cause to be recorded and kept, minutes of all the proceedings of the meetings of the committee and keep the Board informed of the committee's activities, in writing.

(6) A member of a committee shall be paid such remuneration and other allowances, if any, from the funds of the Authority, as the Minister may determine.

(7) The provisions of sections 15, 16, 17, 23 and 24 shall, with the necessary modifications, apply to a member of a committee.

Co-opted members

26. (1) The Board may co-opt any person to attend a meeting of the Board or otherwise assist the Board with its deliberations, and such person shall not have any voting or any rights on the Board.

(2) The provisions of sections 23 and 24 shall, with necessary modifications, apply to co-opted members.

PART V — *Chief Executive Officer and staff of the Authority*

Chief Executive Officer

27. (1) There shall be a Chief Executive Officer of the Authority, who shall be appointed by the Minister, on the recommendation of the Board, and on such terms and conditions as may be specified in the instrument of appointment.

(2) The Chief Executive Officer shall be responsible to the Board.

(3) The Chief Executive Officer shall not, while in the employment of the Authority engage in paid employment outside the duties of his or her office in the Authority.

(4) The Chief Executive Officer shall hold office for a maximum period of five years on such terms and conditions as may be specified in the instrument of appointment, and may be considered for re-appointment for one more term not exceeding five years.

(5) The Chief Executive Officer shall, subject to the directions of the Board on matters of policy, be responsible for —

(*a*) the supervision of the day-to-day affairs of the Authority;

(*b*) ensuring that the Authority is carrying out the functions and duties placed upon it in terms of this Act;

(*c*) running of the Authority on sound commercial and financial principles in accordance with policies and decisions made by the Board;

(*d*) controlling the resources and operations of all the services under the Authority

(*e*) implementing the decisions of the Board; and

(*f*) carrying out any duty that may be conferred on him or her by the Board.

(6) In the performance of his or her duties, the Chief Executive Officer shall keep the Board fully informed of the affairs of the Authority and shall consult the Board from time to time, as may be necessary.

(7) The Chief Executive Officer may delegate to the Secretary, any senior staff or any member of staff of the Authority, as he or she considers appropriate, the exercise of any powers which he or she is authorised to exercise under this Act.

(8) The Minister may, after consultation with the Board, terminate the appointment of the Chief Executive Officer –

(*a*) if the Chief Executive Officer conducts himself or herself in a manner that is detrimental to the objective of, or the proper performance of the functions of the Authority; or

(*b*) if the Chief Executive Officer has been found to be physically or mentally unable to perform his or her duties efficiently, and a medical doctor has issued a certificate to that effect.

(9) The Chief Executive Officer may resign from his or her office by giving 30 days' notice of his or her intention to resign from office, in writing, to the Minister.

Secretary to Board

28. (1) The Board shall, on the recommendation of the Chief Executive Officer appoint a Secretary to the Board (referred to as "the Secretary"), on such terms and conditions as may be specified in the instrument of appointment.

(2) The Secretary shall, in addition to any function that may be assigned to him or her by the Board or the Chief Executive Officer, be responsible for —

(*a*) taking minutes of the meetings of the Board;

(*b*) keeping records of all decisions of the Board; and

(*c*) keeping records of legal transactions of the Authority.

(3) The Secretary shall, unless the Board otherwise directs, in writing, giving the circumstances leading to its decision, attend all meetings of the Board but shall not have a right to vote on any matter before the Board.

(4) In the performance of his or her duties, the Secretary shall be accountable to the Chief Executive Officer.

(5) In the absence of the Secretary, the Chief Executive Officer may appoint any senior member of staff of the Authority to perform the functions of the Secretary until the Secretary resumes office or the vacancy is filled, as the case may be.

Appointment of senior and other staff of Authority

29. (1) The Board shall, on the recommendation of the Chief Executive Officer, appoint the senior staff of the Authority.

(2) The senior staff shall, under the direction of the Chief Executive Officer, assist the Chief Executive Officer in the proper administration and management of the functions and affairs of the Authority, in accordance with the policies laid down by the Board.

(3) The Chief Executive Officer shall appoint such other staff as may be necessary for the proper discharge of the functions of the Authority.

(4) The terms and conditions of employment of staff of the Authority shall be as determined by the Board, in consultation with the Minister.

PART VI — *Financial Provisions*

Funds of Authority

30. (1) The funds of the Authority shall consist of —

(*a*) such monies as may be appropriated by the National Assembly for the purposes of the Authority;

(*b*) such grants and donations as the Authority may receive;

(*c*) such fees as may be charged for services rendered by the Authority;

(*d*) such fees collected as administrative penalties imposed by the Authority;

(*e*) the fees that may be charged by the Authority, for licences under this Act; and

(*f*) any income that the Authority may receive from investments.

(2) Notwithstanding the provisions of subsection (1) (*a*), the moneys to be appropriated by the National Assembly for the purposes of the Authority shall be appropriated for a period not exceeding five years, commencing from the first day of operations of the Authority.

(3) The Authority shall use the revenues acquired under subsection (1) to meet the costs incurred for its operations and shall use any surplus accrued for such purposes as it may determine, with the approval of the Minister.

Strategic and annual plan

31. (1) The Authority shall submit a five-year strategic plan to the Minister, for the Minister's approval, outlining —

(*a*) the goals of the Authority;

(*b*) the objectives of the Authority;

(*c*) the budget of the Authority; and

(*d*) any other matter which the Minister may direct for that five-year period.

(2) The Authority shall, at least three months before the beginning of each year, submit an annual plan to the Minister, for approval outlining —

(*a*) the goals of the Authority;

(*b*) the objectives of the Authority;

(*c*) the budget of the Authority; and

(*d*) any other matter which the Minister may direct for that financial year.

Financial year

32. The financial year of the Authority shall be a period of 12 months, beginning on the 1st April of each year and ending on the 31st March of the subsequent year.

Accounts and audit

33. (1) The Authority shall keep and maintain proper accounts and records of accounts in respect of every financial year relating to its assets, liabilities, income and expenditure, and shall prepare, in each financial year, a statement of such accounts.

(2) The accounts of the Authority in respect of each financial year shall, within three months of the end of the financial year, be audited by an auditor appointed by the Board.

(3) The auditor shall report in respect of the accounts for each financial year, in addition to any other matter on which the auditor deems it pertinent to comment on, whether or not —

(*a*) the auditor has received all the information and explanation which, to the best of the auditor's knowledge and belief, were necessary for the performance of the auditor's duties;

(*b*) the accounts and related records of the Authority have been properly kept;

(*c*) the Authority has complied with all the financial provisions of this Act with which it is its duty to comply with; and

(*d*) the statement of accounts prepared by the Authority was prepared on a basis consistent with that of the preceding year and represents a true and fair view of the transactions and financial affairs of the Authority.

(4) The auditor's report and a copy of the audited accounts shall, within 14 days of completion, be forwarded to the Authority by the auditor.

Pension and other funds

34. (1) The Authority may, out of its revenues, establish and maintain such pension, superannuation, provident or other funds as it may consider desirable or necessary for the payment of benefits or other allowances on the death, sickness, injury, superannuation, resignation, retirement or discharge of its staff and may make rules providing for the payment of money out of its revenues to such funds and providing for contributions to such funds by its staff.

(2) The Authority may contract with insurance companies or such other bodies as may be appropriate for the maintenance and administration of the funds authorised under subsection (1).

Annual report

35. (1) The Authority shall, within a period of six months after the financial year or within such longer period as the Minister may approve, submit, to the Minister, a comprehensive report of its operations during that year, together with the auditor's report and the audited accounts as provided for in section 33 and the report shall be published in such manner as the Minister may require.

(2) The Minister shall lay the annual report of the Authority in Parliament, within three months of its receipt.

PART VII — *Licensing of Cybersecurity Providers*

Licensable cybersecurity services

36. For the purposes of this Act, the following are cybersecurity services that may be licensed in terms of the Act —

(*a*) penetration testing;
(*b*) security operations centre;
(c) information security service;
(*d*) information security risk assessment;
(e) vulnerability assessment;
(*f*) incident response;
(*g*) cyber audit;
(*h*) red teaming;
(*i*) software development; or
(*j*) such other services, as may be prescribed.

Licensing of cybersecurity providers

37. (1) A person shall not provide a cybersecurity service, unless that person obtains a licence granted by the Authority, in accordance with this Act.

(2) A person who seeks to provide a cybersecurity service shall make an application to the Authority in such manner and form, as may be prescribed and such application shall be accompanied by —

(*a*) such fee, as may be prescribed; and

(*b*) such supporting documentation, as may be prescribed.

(3) A person who contravenes the provisions of subsection (1) commits an offence and is liable to a fine of not less than P100 000 but not more than P500 000, or to imprisonment for a term not less than two years but not more than four years, or to both, and in the case of a company, to a fine not exceeding 10 per cent of its annual turnover.

Grant of licence

38. (1) The Authority shall, where the Authority approves an application under section 37, grant the applicant with a licence in such manner and form, as may be prescribed and upon payment of such fee, as may be prescribed.

(2) A licence granted by the Authority shall be subject to such terms and conditions, as may be prescribed.

(3) Where the Authority refuses to grant a licence, the Authority shall communicate such refusal, in writing, within 14 days, giving reason for such refusal.

(4) A licensed cybersecurity service provider who uses a licence granted in terms of this section for a purpose other than that for which the licence was granted, commits an offence and is liable to —

(*a*) a fine not exceeding P200 000 or to imprisonment for a term not exceeding four years, or to both; and

(*b*) in the case of a company, to a fine not exceeding 10 per cent of its annual turnover.

(5) A licence granted in terms of this Act shall expire in accordance with such conditions, as may be prescribed.

Renewal of licence

39. (1) A licensed cybersecurity service provider that intends to renew a licence granted to the service provider in terms of section 38 shall, not less than three months before expiry of the licence, apply for renewal of the licence in such manner and form, as may be prescribed, and upon payment of such fee, as may be prescribed.

(2) The Authority shall renew the licence, if the cybersecurity service provider remains in compliance with the conditions of the licence specified in the licence.

(3) A licence renewed under this section shall be valid for such period, as may be specified in the licence.

(4) A cybersecurity service provider who applies for the renewal of a licence later than the period specified in subsection (1), shall pay such penalty fee for the late application, as may be prescribed.

Assessment of application for licence

40. (1) The Authority shall, within one day of the receipt of an application for a licence in terms of section 37, acknowledge in writing, receipt of the application.

(2) In assessing an application under this Act, the Authority shall consider —

(*a*) whether the grant or renewal of a licence will bring any benefits to the national economy; and

(*b*) whether the applicant can provide the service in respect of which the licence or renewal application is made, in a sustainable manner.

(3) If, after receipt of the application, the Authority is of the opinion that it requires further information to assess the application, the Authority may within such period as may be prescribed, and by written notice, request for further information from the applicant or third parties, as may be identified by the Authority, and the notice shall —

(*a*) specify the information required from the applicant;

(*b*) specify the time within which the information or comments shall be submitted to the Authority; and

(*c*) specify the date by which the Authority intends to make a final decision on the application.

(4) The Authority shall notify an applicant, in writing, of its decision, within such period as may be prescribed, and where the Authority decides not to grant the licence, state the reasons in such notice.

Variation of licence

41. A licensee may, at any time during the validity of the licence, apply to the Authority for a variation of the licence in such manner and form, as may be prescribed, and upon payment of such fee, as may be prescribed.

Non-transferability of licence

42. (1) A licensee shall not transfer a licence granted under this Act to another person.

(2) A licensee who transfers a licence contrary to subsection (1), commits an offence and is liable to —

(*a*) a fine not exceeding P100 000, or to imprisonment for a term not exceeding two years, or to both; and

(*b*) in the case of a company, to a fine not exceeding 10 per cent of its annual turnover.

Suspension of licence

43. (1) The Authority may suspend a licence issued under this Act for a period of not more than six months where —

(*a*) the licensee fails to comply with a condition specified in the licence; or

(*b*) the Authority deems it necessary for the security of the public peace or for public safety to suspend the license.

(2) The Authority shall, before exercising the power of suspension under this subsection (1) (*a*) —

(*a*) give the licensee 14 days' notice, in writing, of the intention to do so; and

(*b*) specify in the notice the grounds on which the Authority intends to suspend the licence.

(3) The Authority shall, with regard to the suspension of a licence in terms of the provisions of subsection 1 (*b*), suspend such licence immediately.

(4) Where the Authority decides to suspend a licence in terms of subsection (1) (*a*), the Authority shall give the licensee the opportunity –

(*a*) to submit to the Authority, within the time specified by the Authority, a written statement of objections, if any, to the suspension of the licence; and

(*b*) to remedy, within the time specified by the Authority, the breach which has occasioned the decision to suspend the licence.

(5) The Authority shall, immediately upon the decision to suspend a licence being made, notify the cybersecurity service provider concerned of the suspension.

(6) Where the Authority decides to suspend the licence of a cybersecurity service provider, the Authority shall by Notice published in the *Gazette*, publish the details of such suspension.

Revocation of licence

44. (1) The Authority may revoke a licence granted under this Act —

(*a*) where a licensee contravenes the provisions of this Act;

(*b*) where the licensee has ceased to carry on the business for which the licensee is licensed;

(*c*) where the licensee has been convicted in Botswana or elsewhere of any offence involving fraud, dishonesty or moral turpitude, cybercrime or breach of privacy laws for which the licensee has not received a free pardon;

(*d*) where the licensee demonstrates a history of repeated or continuous significant deviations from the terms and conditions of the licensee's licence, that represent a breakdown of process controls, rather than isolated incidents; or

(*e*) where the licensee is liquidated or has been declared insolvent by a court.

(2) Where the Authority decides to revoke the licence of a cybersecurity service provider in terms of this section, the Authority shall cause Notice of such revocation, to be published in the *Gazette*.

PART VIII — *Critical Information and Critical National Information Infrastructure*

Designation of critical information and critical national information infrastructure

45. (1) The Authority shall, by Notice in the *Gazette*, designate an information or information infrastructure relevant to a critical sector as a critical information or critical national information infrastructure.

(2) An information or information infrastructure that is designated as critical under subsection (1), shall apply for a licence in such form and manner, as may be prescribed.

(3) Where an information or information infrastructure is designated as critical under subsection (1), the owner of the information or information infrastructure, shall comply with such baseline security requirements, as may be prescribed.

(4) The Authority may by Notice published in the *Gazette*, publish all designated critical information or critical national information infrastructure owners.

Categories of critical information and critical national information infrastructure

46. (1) The Minister may prescribe the categories of critical information and critical national information infrastructure.

(2) The Minister shall, when categorising critical information or critical national information infrastructure under subsection (1), consider the following —

(*a*) the scale of distribution of the impact of any disruption on the critical information or critical national information infrastructure;

(*b*) time criticality in relation to recovery time objective and recovery point objective in connection with any disruption on the critical information or critical national information infrastructure;

(*c*) the cyber dependence of the critical information or critical national information infrastructure; and

(*d*) any other factors that the Authority may consider necessary.

(3) The Authority shall issue guidelines setting out the requirements applicable to the different categories of critical information and critical national information infrastructure.

Registration of critical information and critical national information infrastructure

47. (1) The owner of a critical information or critical information infrastructure shall register a critical information or critical national information infrastructure with the Authority, within 14 days of the designation under section 45, in such manner and form, as may be prescribed.

(2) An owner who contravenes the provisions of subsection (1), commits an offence and is liable to–

(*a*) where the owner is a company, to pay to the Authority an administrative penalty not exceeding 10 per cent of its annual turnover; or

(*b*) where the owner is a natural person, to a fine not exceeding P100 000, or to imprisonment for a term not exceeding two years, or to both.

Withdrawal of designation of critical information and critical national information infrastructure

48. The Authority may by, Notice published in the *Gazette*, withdraw the designation of a critical information or critical national information infrastructure at any time, if the Authority considers that information or information infrastructure no longer satisfies the criteria of a critical information or critical national information infrastructure.

Hosting of critical information and critical national information infrastructure

49. (1) An owner of a critical information or critical national information infrastructure shall host critical information or critical national information infrastructure within Botswana, in such manner and form, as may be prescribed.

(2) Notwithstanding the provisions of subsection (1), the Authority may authorise an owner to host critical information or critical national information infrastructure outside Botswana.

(3) The Authority shall, before authorising the hosting of critical information or critical national information infrastructure outside Botswana under subsection (2), consider the following factors –

(*a*) the categories of critical information or critical national information infrastructure referred to under section 46;
(*b*) the justification of hosting the critical information or critical national information infrastructure outside Botswana;
(*c*) the nature of business operations;
(*d*) the need to maintain national cyber resilience;
(*e*) whether the proposed hosting country has a legal framework on cybersecurity that would facilitate the regulation of the critical information or critical national information infrastructure;
(*f*) whether the critical information or critical national information infrastructure belongs to a public body;
(*g*) issues of national security;
(*h*) the categories of personal data required to be stored within Botswana in terms of the Data Protection Act; and
(*i*) any other factors, as may be prescribed.

(4) Where the purpose for which critical information was collected expires or the owner ceases to exist, the critical information shall be surrendered to the Authority.

(5) Where a critical information surrendered under subsection (4) is personal data, that data shall be dealt with in accordance with the Data Protection Act.

Change in ownership of critical information and critical national information infrastructure

50. (1) An owner of a critical information or critical national information infrastructure shall seek the approval of the Authority, in such form and manner as may be prescribed, of any change of ownership of critical information or critical national information infrastructure within seven days of the change, in such manner and form, as may be prescribed.

(2) An owner who contravenes the provisions of subsection (1), commits an offence and is liable to —

(*a*) where the owner is a company, to pay to the Authority an administrative penalty not exceeding 10 per cent of its annual turnover; or
(*b*) where the owner is a natural person, to a fine not exceeding P100 000, or to imprisonment for a term not exceeding two years, or to both.

Auditing of critical information and critical national information infrastructure

51. (1) The Authority shall carry out a periodic audit and inspection on critical information and critical national information infrastructure to ensure compliance with the provisions of this Act.

(2) The Minister may prescribe the minimum standards for the general management of critical information and critical national information infrastructure, that the Minister considers necessary for the protection of national security.

(3) Subject to the provisions of subsection (1), an audit conducted under subsection (1) may be performed by an independent auditor appointed by the Authority.

Non-compliance to audit requirements

52. (1) The Authority shall, notify an owner in writing, where an audit conducted under section 51 does not comply with the prescribed standards under this Act, stating the —

(*a*) findings of the audit;

(*b*) action required to remedy the non-compliance; and

(*c*) period within which the owner shall take remedial action.

(2) An owner who fails to take any remedial action within the period stipulated under subsection (1), commits an offence and is liable to —

(*a*) where the owner is a company, to pay to the Authority an administrative penalty not exceeding 10 per cent of its annual turnover; or

(*b*) where the owner is a natural person, to a fine not exceeding P100 000 or to imprisonment for a term not exceeding two years, or to both.

Duty to report cybersecurity incidents in respect of critical information and critical national information infrastructure

53. (1) An owner of a critical information or critical national information infrastructure shall, immediately notify the Botswana Computer Security Incident Response Team, established under section 54, of a perceived or actual occurrence of any of the following cybersecurity incidences, in such manner that the Botswana Computer Security Incident Response Team may determine —

(*a*) a cybersecurity incident in respect of critical information or critical national information infrastructure;

(*b*) a cybersecurity incident in respect of any computer, computer system or information system under the owner's control that is interconnected or communicates with critical information or critical national information infrastructure; or

(*c*) any other type of cybersecurity incident in respect of critical information or critical national information infrastructure that the Botswana Computer Security Incident Response Team may specify to the owner.

(2) Notwithstanding the provisions of subsection (1), an owner shall submit a preliminary cybersecurity incident report to the Botswana Computer Security Incident Response Team, immediately after the incident is detected and within a period of not more than eight hours of notifying the Botswana Computer Security Incident Response Team of the perceived or actual occurrence of the incident under that subsection, in such manner and form, as may be prescribed.

(3) An owner shall, as soon as the cybersecurity incident is resolved, submit to the Botswana Computer Security Incident Response Team, a detailed cybersecurity incident report.

(4) An owner shall establish mechanisms and processes, in accordance with such cybersecurity standards as may be prescribed, for the detection of a cybersecurity threat in respect of critical information or critical national information infrastructure.

(5) An owner who contravenes the provisions of this section, commits an offence and is liable to —

(*a*) where the owner is a company, pay to the Authority an administrative penalty not exceeding 10 per cent of its annual turnover; or

(*b*) where the owner is a natural person, a fine not exceeding P100 000 or to imprisonment for a term not exceeding two years, or to both.

PART IX — *Botswana Computer Security Incident Response Team*

Establishment of Botswana Computer Security Incident Response Team

54. (1) The Authority shall establish the Botswana Computer Security Incident Response Team.

(2) The Botswana Computer Security Incident Response Team shall promote cybersecurity and cyber resilience and the protection of the critical information and critical national information infrastructure.

(3) Without derogating from the generality of subsection (2), the Botswana Computer Security Incident Response Team shall —

(*a*) act as Botswana's centralised point of contact for cybersecurity incident reporting, coordination and international cooperation on cybersecurity threats and incidents;

(*b*) monitor cybersecurity threats and incidents;

(*c*) disseminate and share information, alerts, security advisories and threats intelligence;

(*d*) provide computer security incident response support at national level;

(*e*) carry out joint simulation exercises and cyber drills with stakeholders to enhance national preparedness;

(*f*) raise public education and awareness in the field of cybersecurity;

(*g*) provide incident response and management services in a coordinated manner through established industry standard policies and procedures to manage threats associated with cyber incidents;

(*h*) at the request of the Government, represent Botswana in international regulatory and other fora concerning cyber incident response teams;

(*i*) establish a cybersecurity incident monitoring and response system;

(*j*) assess and coordinate the work of sectoral cyber incident response teams within the public and private sector;

(*k*) develop and review National Contingency Plans;

(*l*) carry out national cybersecurity preparedness exercises annually or as and when necessary; and

(*m*) perform such other functions, as may be prescribed.

(4) The Botswana Computer Security Incident Response Team shall submit to the Authority, a monthly report covering the operations of the Botswana Computer Security Incident Response Team.

(5) The Botswana Computer Security Incident Response Team shall implement response and recovery actions that follow the standards and protocols as determined by the Authority, for such action.

(6) The Botswana Computer Security Incident Response Team shall, upon the request of the Authority, submit an incidence report to the Authority.

(7) An incidence report prepared by the Botswana Computer Security Incident Response Team, in terms of subsection (6) shall not be shared with any third party, except in the fulfillment of a court order.

(8) The Botswana Computer Security Incident Response Team shall submit a bi-annual State of Cybersecurity in Botswana Report to the Authority.

Sectoral cyber incident response teams

55. (1) The Authority shall establish such sectoral cyber incident response teams, as it may determine.

(2) The Authority shall, in establishing a sectoral cyber incident response team, take into account —

(*a*) the needs and criticality of a sector;

(*b*) developments in respect of cybersecurity in Botswana; and

(*c*) any other factors that the Authority may determine.

(3) A sectoral cyber incident response team shall –

(*a*) collect and collate cybersecurity incidents; and

(*b*) coordinate responses to cybersecurity incidents within its specific sector.

(4) The establishment and operational costs of a sectoral cyber incident response team, shall be borne by the sector concerned.

(5) The Authority shall oversee the operations of a sectoral cyber incident response team constituted under this section.

(6) A sectoral cyber incident response team shall submit a report on the operations of that sectoral cyber incident response team to the Authority, in such manner as may be determined by the Authority.

Duty to report cybersecurity incident

56. (1) A sectoral cyber incident response team shall report a cybersecurity incident to the Botswana Computer Security Incident Response Team.

(2) A licensee under this Act shall, within the period determined by the Authority, submit to the Botswana Computer Security Incident Response Team, a report covering the operations of the licensee, including a report of a cybersecurity incident.

(3) The Authority shall establish a cybersecurity incident reporting and information sharing platform to enable the Botswana Computer Security Incident Response Team, a sectoral cyber incident response team, a licensee and any other relevant institution to report a cybersecurity incident.

(4) The Botswana Computer Security Incident Response Team shall, upon receipt of information in respect of a cybersecurity incident, circulate the information to the Botswana Computer Security Incident Response Team, a sectoral cyber incident response team, a licensee and any other relevant institution.

(5) An owner of a critical information and critical national information infrastructure shall report a cybersecurity incident to the relevant sectoral cyber incident response team or the Botswana Computer Security Incident Response Team, immediately after the incident is detected and within a period of not more than eight hours.

(6) An owner person who contravenes the provisions of subsection (5) commits an offence and is liable to —

(*a*) where the owner is a company, an administrative penalty not exceeding 10 per cent of its annual turnover;

(*b*) where the owner is a natural person, a fine not exceeding P250 000 or to imprisonment for a term not exceeding three years, or to both.

Cybersecurity incident monitoring and response system

57. (1) The Authority shall establish a cybersecurity incident monitoring and response system.

(2) The Authority shall implement the relevant technical measures to ensure an effective cybersecurity incident monitoring and response system.

(3) For the purposes of subsection (2), the Authority shall intercept, disable or take-down a digital technology, digital service or a digital product that is likely to undermine the cybersecurity of Botswana.

(4) The Authority shall monitor cybersecurity threats, whether such cybersecurity threats occur in or outside Botswana.

Early warning system

58. (1) The Authority shall establish an early warning system in respect of human initiated risks that are likely to undermine the cybersecurity of Botswana.

(2) The Authority shall implement the early warning system to advise the public on cybersecurity matters.

PART X — *International Cooperation*

International cooperation
Cap. 08:04
Cap. 09:03

59. (1) Subject to the provisions of the Mutual Assistance in Criminal Matters Act and the Extradition Act, the Authority shall in the performance of its functions promote the security of the cyberspace through international cooperation.

(2) The Authority shall identify and ensure that it cooperates with private bodies, organisations and Government entities involved in cybersecurity matters, within and outside the Botswana.

(3) For the purposes of international cooperation, the Authority shall be the 24/7 contact point to tackle cybersecurity threats and incidents.

(4) The Botswana Computer Security Incident Response Team shall provide assistance in respect of technical advice to other contact points, including law enforcement bodies.

(5) Subject to the Mutual Assistance in Criminal Matters Act, the Authority may enter into an agreement with a foreign country or international body relating to the provision of mutual assistance and cooperation in the investigation and prosecution of —

(*a*) an offence committed under this Act;
(*b*) any offence under the laws of Botswana which is or was committed by the use of a device or computer related article; or
(*c*) an offence substantially similar to an offence recognised in Botswana which is or was committed by the use of a device or computer related article, in the foreign country.

PART XI — *Miscellaneous Provisions*

Registers

60. (1) The Authority shall establish and maintain —
(*a*) an electronic cybersecurity risk register; and
(*b*) a register of regulatory documents.
(2) The cybersecurity register shall contain —
(*a*) details of the —
(i) personal data of the owners of critical information and critical national information infrastructure,
(ii) identified and potential cybersecurity risks,
(iii) level of impact of risk; and
(*b*) such other details, as may be prescribed.
(3) Information contained in the cybersecurity risk register shall not be disclosed to any person other than an employee of the Authority, who is responsible for keeping the register.
(4) Notwithstanding the provisions of subsection (3), the Authority may disclose information contained in the cybersecurity risk register, if required by law.
(5) Nothing in this law shall preclude the Authority from pleading in proceedings relating to information held in the custody or records of the Authority that the production or disclosure of that information may be —
(*a*) prejudicial to the security of the State; or
(*b*) injurious to the public interest.
(6) The register of regulatory documents shall be made available to members of the public at the principal office of the Authority during its normal office hours and at its regional offices.
(7) The register of regulatory documents shall contain such matters, as may be prescribed.

Request for information

61. (1) The Authority may, in writing, direct —
(*a*) a person who owns or operates a critical information or critical national information infrastructure;
(*b*) a designated sectoral computer emergency response team; or
(*c*) a cybersecurity service provider,
to provide the Authority with relevant information for the purpose of ensuring the cybersecurity of Botswana.
(2) A person who fails to provide information in terms of subsection (1), commits an offence and is liable to pay to the Authority an administrative penalty of P250 000.

(3) For a second or subsequent offence, the person is liable to pay to the Authority, an administrative penalty of P500 000.

Exemption from liability of officers of Authority and members of Board

62. A member of the Board and an officer of the Authority shall be exempt from liability for any action taken or omission made in good faith, in the performance of the functions of the Authority.

Review of decisions of Authority

63. A person aggrieved by the decision of the Authority may within 90 days of the decision, apply for a review of the decision of the Authority, to the High Court.

Codes of practice and standards

64. (1) The Authority may issue codes of practice and standards as may be necessary for the better carrying out of the provisions of this Act.

(2) The Authority shall publish the codes of practice and standards on the Authority's website, in a daily newspaper of general circulation in Botswana, the *Gazette* or any other electronic platform.

(3) The codes of practice and standards issued by the Authority under this Act shall bind all persons regulated under this Act and may include codes of practice and standards relating to —

(*a*) cyber incident reporting;
(*b*) cybersecurity;
(*c*) cyber resilience;
(*d*) critical information and critical national information infrastructure risk assessments;
(*e*) critical information and critical national information infrastructure data retention;
(*f*) cyber incident management exercises; and
(*g*) the identification of critical national information infrastructure.

Exemptions

65. (1) The Authority may, by Notice published in the *Gazette*, exempt a person or class of persons, for a limited or unlimited period of time, from the requirements of the provisions of Parts VII and VIII.

(2) The Authority may, under any circumstances as it may determine, revoke the exemption granted to any person in terms of subsection (1).

(3) The Authority may where it revokes its decision under subsection (2), publish the decision by Notice in the *Gazette*.

Regulations

66. (1) The Minister may, after consultation with the Authority, make regulations for the better carrying out of the provisions of this Act.

(2) Without prejudice to the generality of the powers conferred by subsection (1), the regulations may provide for —

(*a*) the form and manner of making applications for licences under this Act, the renewal of licences or variation of the licences, the duration of the licences granted under this Act, conditions under which licenses under this Act may be granted and the fees payable for such licences;
(*b*) the period for assessment of applications for licences;
(*c*) the manner and form of registration of critical information and critical national information infrastructure;

(*d*) the baseline requirements for critical information and critical national information infrastructure;
(*e*) categories of critical information and critical national information infrastructure;
(*f*) the form of notification to be given by a licensee where there is a change in the ownership of a critical information and critical national information infrastructure;
(*g*) categories of licences of cybersecurity services;
(*h*) manner of hosting of critical information and critical national information infrastructure;
(*i*) the factors to be considered for the hosting of critical information and critical national information infrastructure outside Botswana;
(*j*) the categories of cybersecurity services that may be licensed under this Act;
(*k*) the manner and form for the application for registration of an interception device; and
(*l*) provide for anything required to be prescribed under this Act.

PASSED by the National Assembly this 14th day of August, 2025.

DR. GABRIEL G. G. MALEBANG,
Clerk of the National Assembly.

(4) The members of the committee who are members of the Board may take part in the proceedings of the committee, but shall not have the right to vote.

(5) Subject to the directions of the Board, a committee established under this section may regulate its own procedure.

(6) Unless in appointing any such committee the Board has appointed a Chairperson, the committee shall elect one of its members as a Chairperson of the committee.

(7) The Board may revoke or amend any delegation made under the provisions of subsection (1) and may attach conditions to such delegation, including general or particular directions, as to the manner in which any delegated power is to be exercised.

PART VI — *Offences*

Anti-doping rule violation

22. An athlete or any other person who is to participate, or has participated in any sport event in Botswana or outside Botswana may be found to have committed an anti-doping rule violation if it is established that he or she has committed one or more of the violations for doping in sport set out in the Code.

Penalties

23. An athlete or any other person who is to participate or has participated in any sport event in Botswana or outside Botswana, who commits an anti-doping rule violation as may be prescribed in the Code may —

(*a*) have his or her results disqualified with all consequences, including forfeiture of medals, points and prizes, in such a manner as may be prescribed in the Code;

(*b*) be ineligible to participate in any competition, event, or other activity or funding, for such period and in such a manner as may be prescribed in the Code;

(*c*) receive provisional suspension from participating in any competition or activity prior to a final decision being taken in a hearing; or

(*d*) be subject to any other consequence prescribed in the Code.

PART VII — *Anti-Doping Activities*

Therapeutic use exemption

24. (1) Where any substance or method is included in the prohibited list and such prohibited substance or prohibited method is required for use by an athlete for therapeutic reasons, such athlete may apply in such form as may be determined in the anti-doping rules, the Code and the International Standard for Therapeutic Use Exemptions (ISTUE), to the Organisation, for granting therapeutic use exemption in respect of such prohibited substance or prohibited method.

(2) An application under subsection (1) shall be made —

(*a*) as soon as reasonably possible after the athlete becomes aware that the use of a prohibited substance or prohibited method is required; and

(*b*) subject to any circumstance of emergency or exceptional situation, no later than 30 days prior to the participation of the athlete in any competition or event.

(3) The Organisation may consider the application received by it under subsection (1) in such a manner and after taking into consideration such criteria and procedure as it shall be determined in the anti-doping rules, the Code and the international standard for therapeutic use exemption.

(4) The Organisation shall, either grant or refuse to grant therapeutic use exemption with regards to an application received under subsection (1), in such a manner as shall be determined in the Code and the international standard for therapeutic use exemptions.

Report of violation

25. A person may report any information suggesting or relating to an anti-doping rule violation by an athlete or athlete support personnel or any other person to the Director-General.

Powers of entry, search and seizure

26. (1) Where the Organisation has reason to believe that an athlete or athlete support personnel or any other person to whom this Act applies has committed an anti-doping rule violation, the Organisation may authorise the entry and search of the athlete, athlete support personnel or any other person's premises by an inspector appointed in writing by the Organisation to —

(*a*) enter into a place, with such assistance as may be considered necessary, for the purpose of inspecting, examining and determining if any anti-doping rule violation has been committed or is being committed;

(*b*) search any premises in which the inspector has reason to believe that any anti-doping rule violation has been, or is being, or is about to be committed; and

(*c*) seize any equipment, device, substance, record, register, document or other material object, if such inspector believes that it may furnish evidence of such anti-doping rule violation or that seizure is necessary to prevent or mitigate any anti-doping rule violation.

(2) An authorised inspector may be accompanied by a police officer in the conduct of his or her duties under subsection (1).

Powers to test

27. As part of routing doping control, the Organisation shall require athletes to submit to testing, in such a manner and procedure as may be prescribed under the Code and international standard for testing and investigations.

WADA Accredited laboratories

28. (1) The Organisation shall cause a sample taken from an athlete to be analysed at an accredited laboratory or a laboratory approved by the World Anti-Doping Agency to detect presence of prohibited substances or its metabolites and markers in an athlete's sample or the use of a prohibited method.

(2) A sample, related analytical data or doping control information shall be analysed —

(*a*) to detect prohibited substances and prohibited methods identified on the prohibited list and other substances as may be directed by the World Anti-Doping Agency;

(*b*) to assist the Organisation in profiling relevant parameters of an athlete's sample, including for deoxyribonucleic acid or genomic profiling; or

(*c*) for any other legitimate anti-doping purpose.

(3) The results of all tests sample analysis shall be submitted to the Organisation.

Result management process

29. (1) The Organisation shall, after receiving a report from the World Anti-Doping Agency accredited or approved laboratory indicating the presence of any prohibited substance or its metabolites or markers in the sample of an athlete, carry out initial examination of the report in such a manner as may be determined in the Code or in the applicable international standards.

(2) Where the Organisation identifies the presence of a prohibited substance or its metabolites or markers, or the use of a prohibited method in the sample of an athlete, it shall determine whether or not therapeutic use exemption has been granted to such athlete in respect of such substance.

(3) Where the Organisation is satisfied that no therapeutic use exemption has been granted to the athlete, and that no departure from any international standard caused the presence of the prohibited substance or its metabolites or markers in the athlete's sample, it shall take such actions and, in such manner, as may be determined by the Code and relevant and applicable international standards.

PART VIII — *General Provisions*

Indemnity

30. No matter or thing done by a member of the Board, a member of staff of the Organisation or any person authorised by the Board or the Organisation shall, if the matter or thing is done *bona fide* in the course of the operations of the Organisation, render the member, member of staff or authorised person, personally liable to an action, claim or demand.

Offences

31. (1) A person who —

(*a*) fails to comply with any lawful order or direction of the Organisation;

(*b*) presents to the Organisation a false document or makes a false statement with the intent to deceive or mislead an investigating officer or inspector; or

(*c*) willfully obstructs or hinders any person acting in the performance of any function or exercise of powers conferred by this Act, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both.

(2) A health practitioner or a person registered under a recognised health professions regulatory body, or any other health related professional who —

(*a*) prescribes or dispenses prohibited substances or methods to an athlete with the intent of doping;

(*b*) without justification, administers prohibited substances or methods to an athlete;