THE CYBER SECURITY ACT, 2025

ARRANGEMENT OF SECTIONS

GOVERNMENT OF ZAMBIA

ACT

No. 3 of 2025

Date of Assent: 8th April, 2025

An Act to provide for cyber security in the Republic; establish the Zambia Cyber Security Agency and provide for its functions; provide for the regulation of cyber security service providers; provide for the constitution of the Zambia Cyber Incident Response Team and provide for its functions; provide for the constitution of sectoral cyber incident response teams; continue the existence of the Central Monitoring and Co ordination Centre; provide for the designation, protection and registration of critical information and critical information infrastructure; repeal and replace the Cyber Security and Cyber Crimes Act, 2021; and provide for matters connected with, or incidental to, the foregoing.

[15th April, 2025

ENACTED by the Parliament of Zambia. Enactment

PART I

PRELIMINARY PROVISIONS

1. This Act may be cited as the Cyber Security Act, 2025, and shall come into operation on the date appointed by the President by statutory instrument. Short title and commencement

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

"access" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"Agency" means the Zambia Cyber Security Agency established under section 3;

"article" means a computer, computer data, computer program, computer data storage medium or computer system which—

(a) on reasonable grounds, is believed to be concerned with, or connected with the commission of a crime or suspected commission of a crime;

(b) may afford evidence of the commission, or suspected commission of a crime; or

(c) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission of a crime;

"Authority" means the Zambia Information and Communications Technology Authority established under the Information and Communication Technologies Act, 2009;

Act No. 15 of 2009

Act No. 7 of 2017

"bank" has the meaning assigned to the word in the Banking and Financial Services Act, 2017;

"call-related information" means data or details that are associated with a telephone call or communication session and includes—

(a) switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment of each communication generated or received by a customer or user of any equipment;

(b) a facility or service provided by a service provider; or

(c) where applicable, the location of the user within the telecommunications system;

"Centre" means the Central Monitoring and Co-ordination Centre continued under section 21;

"certificate of registration" means a certificate of registration issued under section 24;

"communication" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of 2021

"communications data" means information relating to the usage of an electronic communications service;

"computer" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"computer data" means a representation of facts, concepts or information in a form suitable for processing in a computer or computer system, including a program suitable to cause a computer or computer system to perform a function;

"computer data storage medium" means a device or medium used for storing and retrieving digital data or information from a computer;

"computer system" means a set of integrated devices that input, output, process and store data and information including the internet;

"controller" means a person who controls or is responsible for critical information or critical information infrastructure that is registered under this Act;

"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 information infrastructure or processed by a controller;

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

(c) information needed to operate critical information infrastructure; or

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

"critical information infrastructure" means a computer system, device, network, computer program or computer data that—

(a) is vital to a country such that the incapacity or destruction of, or interference with, the computer system, device, network, computer program or computer data would have a debilitating impact on national security, economy, public health or safety; or

(b) supports the processing of critical information or an essential service;

"cyber attack" means malicious activities targeting the confidentiality, integrity or availability of computer systems, computer data or services rendered by computer systems;

"cyber audit" means a third party audit of an organisation's cyber security practices, involving the assessment of that organsation's information security management system, penetration testing and vulnerability assessments for purposes of identifying and mitigating cyber security risks;

"Cyber resilience" means the ability to prepare for, respond to and recover from cyber attacks, ensuring that essential functions continue despite adverse conditions;

"cyber security" means tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies used to protect the cyber environment, organisation and user assets;

"cyber security incident" means an unauthorised activity or event which may result in jeopardising or adversely impacting the confidentiality, availability or integrity of information, a computer, a computer system or a network;

"Cyber Security Risk Register" means the Cyber Security Risk Register kept and maintained under section 20;

"cyber security service" means a service listed under section 41;

"cyber security threat" means a potential danger or risk to a computer, computer system, network, or data that may imminently jeopardise or affect adversely, without lawful authority, the cyber security of that computer, computer system or network or another computer, computer system or network;

"cyber security risk assessment" means the process of identifying, analysing, and evaluating potential threats and vulnerabilities in an information system, network or asset;

"cyber security service provider" means a person licensed under section 45 to provide a cyber security service;

"device" means a unit of physical or virtual hardware or equipment that provides one or more computing functions and includes a computer program, application, a component of a computer system, a computer storage component, an input or output device, or an apparatus which can be used to intercept a wire or electronic communication;

"digital forensics" means the practice of collecting, analysing, and preserving electronic data in a manner that maintains electronic data's integrity and reliability, and is admissible as evidence in a court of law;

"Director-General" means the person appointed as Director-General under section 5;

"electronic communication" has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"electronic communications service" has the meaning assigned to the words in the Information and Communication Technologies Act, 2009; Act No. 15 of 2009

"electronic communications system" has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"electronic communications service provider" means a person licensed to provide an electronic communications service under the Information and Communication Technologies Act, 2009; Act No. 15 of 2009

"essential service" means a service that is fundamental to the operation of society, ensuring public safety, health, economic stability, national security, international order and the maintenance and recovery of critical cyber space infrastructure;

"financial institution" has the meaning assigned to the words in the Banking and Financial Services Act, 2017; Act No. 7 of 2017

"fit and proper person" means a person who is of good character, honest, possesses financial integrity, probity, personal integrity, is of good repute, competent, capable and dependable;

"geolocation" means the process or technique of identifying the geographical location of a person or device by means of digital information processed through the internet;

Act No. 4 of 2021

"hosting" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

"information security audit" means a comprehensive evaluation of information security practices including physical, administrative and technical controls that ensures overall data privacy protection, cyber security, cyber resilience and regulatory compliance;

"inspector" means a person appointed as a cyber security inspector under section 55;

"interception" means an act by a person who is not party to an electronic communication of listening to, monitoring, viewing, reading or recording a private communication in transit, without the knowledge of the person making and receiving the communication, whether such communication is done in real time or otherwise between—

(a) persons;

(b) a person and a device; or

(c) devices;

"internet connection record" means a record which contains information about internet connections made by a particular device and includes—

(a) connections which are made automatically by a person, browser or device;

(b) a customer account reference such as an account number or identifier of the customer's device or internet connection;

(c) a time stamp of a session log;

(d) source and destination internet protocol addresses and the associated identity information;

(e) the volume of data transferred in either or both directions;

(f) the name of the internet service or the server that the service is connected to;

(g) elements of a universal resource locator which constitutes communications data; or

(h) any other related meta data;

"information infrastructure" means communication networks and their associated software that support interaction among people and organisations;

"information system" has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"information technology auditor" means a person who possesses the expertise to examine and evaluate an information security management system as it relates to information technology infrastructure;

"judge" means a judge of the High Court;

"law enforcement officer" means—

(a) a police officer;

(b) an officer of the Anti Corruption Commission;

(c) an officer of the Drug Enforcement Commission;

(d) an officer of the Zambia Security Intelligence Service;

(e) an officer of the National Anti-Terrorism Centre; and

(f) any other person that the President may, by statutory instrument, designate for purposes of this Act;

"legally disqualified" means the absence of legal capacity as provided under section 4 of the Mental Health Act, 2019; Act No. 6 of 2019

"licence" means a licence issued under section 45;

"licensee" means a person licensed under this Act;

"monitor" means to observe and analyse digital activities including network traffic, system logs, or user behaviour, with the goal of detecting and preventing cyber security threats or cyber security incidences;

"orally" means communication or transmission of information through spoken words whether delivered in person, via real time conversation through recorded media or text based formats that capture the essence of communication;

"penetration testing" means assessing, testing or evaluating the cyber security of a computer or computer system and the integrity of any information stored in or processed by the computer or computer system, by searching for vulnerabilities in, and compromising, the cyber security defences of the computer or computer system with express permission of the system owner;

"personal data" has the meaning assigned to the words in the Data Protection Act, 2021;

Act No. 3 of 2021

"private communication" means an electronic communication which is reasonable for the sender or the intended recipient to expect that the communication shall not be intercepted;

"repealed Act" means the Cyber Security and Cyber Crimes Act, 2021 repealed under section 74;

Act No. 2 of 2021

"service provider" means an entity authorised to—

(a) provide or offer an electronic communications system;

(b) process or store computer data on behalf of an electronic communications service provider or user of such service; or

(c) own an electronic communications system to provide or offer an electronic communications service;

"Staff Board" means the Staff Board Constituted in the Schedule;

"Zambia Cyber Incident Response Team" means the Zambia Cyber Incidence Response Team constituted under section 6; and

"Zambia Security Intelligence Service" means the Zambia Security Intelligence Service continued under the Zambia Security Intelligence Service Act, 1998.

Act No. 14 of 1998

PART II

THE ZAMBIA CYBER SECURITY AGENCY

Establishment of Zambia Cyber Security Agency

3. (1) There is established the Zambia Cyber Security Agency in the Office of the President which is responsible for the administration of this Act under the general direction of the President.

(2) The Agency shall be responsible for the coordination of cyber security matters in the Republic.

(3) The Agency shall collaborate with relevant institutions which are constitutionally mandated to defend the Republic in cyber warfare and offensive cyber operations to uphold the sovereignty of the Republic.

Functions of Agency

Act No. 14 of 1998

4. The functions of the Agency are to—

(a) subject to the Zambia Security Intelligence Service Act, 1998, coordinate activities relating to cyber security and cyber resilience;

(b) take measures in response to cyber security incidents which may threaten critical information, critical information infrastructure or any information or infrastructure in the Republic likely to be affected by a cyber security incident;

(c) disseminate information on cyber threats and vulnerabilities;

(d) identify and ensure the protection of critical information and critical information infrastructure;

(e) establish codes of practice and standards for cyber security and monitor compliance with the codes of practice and standards by controllers;

(f) issue licences for the provision of cyber security services;

(g) regulate the conduct of cyber security service providers;

(h) promote and undertake research and development relating to cyber security;

(i) promote and undertake capacity building, education and awareness activities on matters relating to cyber security;

(j) undertake information security audits on critical information and critical information infrastructure;

(k) adopt standards for cyber security products and services and certify cyber security products and services;

(l) develop and implement a national cyber security response plan;

(m) undertake digital forensics;

(n) provide technical assistance and collaborate with other relevant national and international institutions in matters relating to this Act; and

(o) advise the President on matters relating to cyber security.

Director-General and other staff

5. (1) The President shall, appoint a Director-General of the Agency who shall be a public officer.

(2) The Director-General is the chief executive officer of the Agency and is responsible for the day to day management of the Agency.

(3) The President shall appoint a Deputy Director-General, Directors and Deputy Directors who are necessary for the implementation of the provisions of this Act.

(4) The Director-General shall, on the recommendation of the Staff Board, appoint other officers below the rank of Deputy Director that are necessary for the implementation of the provisions of this Act.

PART III

Cyber Incident Response Teams

Zambia Cyber Incident Response Team

6. (1) The Agency shall constitute the Zambia Cyber Incident Response Team which shall—

(a) be the first point of contact with reference to the handling of cyber incidents and communication between local, regional and international cyber security incident response teams;

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

(c) provide alerts and warnings on the latest cyber threats and vulnerabilities which may impact the public and the private sector;

(d) undertake national cyber security risk assessments;

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

(f) participate in regional and international computer emergency response team groups; and

(h) establish a cyber security incident monitoring and response system.

(2) The Agency shall determine the composition, terms of reference, tenure and procedures of the Zambia Cyber Incident Response Team.

Constitution of sectoral cyber incident response teams

7. (1) The Agency shall, by notice in the *Gazette,* require a sector to constitute a sectoral cyber incident response team.

(2) The notice referred to under subsection (1), shall specify—

(a) the composition of the sectoral cyber incident response team; and

(b) the institution to coordinate the sectoral cyber incident response team.

(3) The Agency shall, in requiring a sector to constitute a sectoral cyber incident response team, take into account—

(a) the needs and criticality of a sector;

(b) developments in respect of cyber security in the Republic; and

(c) any other factors that the Agency may determine.

(4) A sectoral cyber incident response team shall—

(a) collect and collate cyber security incidents; and

(b) co-ordinate responses to cyber security incidents within the sectors.

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

(6) A sectoral cyber incident response team shall bear the cost of establishing and operationalising that cyber incident response team.

(7) A sectoral cyber incident response team shall submit a report on the operations of that sectoral cyber incident response team to the Agency in a manner determined by the Agency.

PART IV

PROTECTION OF CRITICAL INFORMATION AND CRITICAL INFORMATION INFRASTRUCTURE

Critical sector

8. For the purposes of this Part, a critical sector includes—

(a) defence and security;

(b) public sector;

(c) banking and finance;

(d) health;

(e) transport;

(f) pensions and insurance;

(g) information and communications technology;

(h) energy;

(i) education;

(j) mining; and

(k) any other sector as may be prescribed.

Designation of critical information or critical information infrastructure

9. (1) The Agency shall, by notice in the *Gazette*, designate information or information infrastructure relevant to a critical sector as critical information or critical information infrastructure.

(2) Where information or information infrastructure is designated as critical under subsection (1), a controller shall comply with the baseline security requirements as may be prescribed.

Categories of critical information and critical information infrastructure

10. (1) There shall be categories of critical information and critical information infrastructure that the Agency may determine.

(2) The Agency shall, when categorising critical information or critical 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 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 information infrastructure;

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

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

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

Registration of critical information and critical information infrastructure

11. (1) A controller shall register critical information or critical information infrastructure with the Agency, within thirty days of the designation under section 9, in a prescribed manner and form.

(2) A controller who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Hosting of critical information and critical information infrastructure

12. (1) A controller shall host critical information or critical information infrastructure within the Republic, in a prescribed manner and form.

(2) Despite subsection (1), the Agency may authorise a controller to host critical information or critical information infrastructure outside the Republic.

(3) The Agency shall, before authorising the hosting of critical information or critical information infrastructure outside the Republic under subsection (2), consider the following factors:

(a) the categories of critical information or critical information infrastructure referred to under section 10;

(b) the justification of hosting the critical information or critical information infrastructure outside the Republic;

(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 cyber security that would facilitate the regulation of the critical information or critical information infrastructure;

(f) whether the critical information or critical information infrastructure belongs to a public body;

(g) national security;

(h) the categories of personal data required to be stored within the Republic under the Data Protection Act, 2021; and

Act No. 3 of 2021

(i) any other factors as may be prescribed.

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

(5) Where critical information surrendered under subsection (4) is personal data, that data shall be dealt with in accordance with the Data Protection Act, 2021.

Act No. 3 of 2021

Change in ownership of critical information or critical information infrastructure

13. (1) A controller shall notify the Agency of any change of ownership of critical information or critical information infrastructure within seven days of the change in the prescribed manner and form.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Auditing of critical information or critical information infrastructure

14. (1) A controller shall annually appoint an information technology auditor to perform a cyber audit on critical information or critical information infrastructure in a manner determined by the Agency.

(2) Despite subsection (1), the Agency may, by notice, require a controller to perform a cyber audit on critical information or critical information infrastructure within a period specified in the notice.

(3) The fees for the cyber audit shall be paid by the controller.

(4) A controller shall submit to the Agency, a report of the cyber audit conducted under subsection (2), within a period as the Agency may determine.

(5) A controller who contravenes this section commits an offence and is liable, on conviction, to a fine not exceeding three million penalty units.

Non-compliance to cyber audit requirements

15. (1) The Agency shall, notify the controller in writing, where a cyber audit does not comply with the guidelines issued relating to cyber audit requirements and this Act, stating the—

(a) findings of the cyber audit;

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

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

(2) A controller who fails to take any remedial action within the period stipulated under subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Report on cyber security situational awareness

16. A controller shall submit to the Agency, a report on cyber security situational awareness in a manner determined by the Agency.

Duty to report cyber security incidents in respect of critical information and critical information infrastructure

17. (1) A controller shall immediately notify the Agency of a perceived or actual occurrence of any of the following cyber security incidences, in a manner that the Agency may determine:

(a) a cyber security incident in respect of critical information or critical information infrastructure;

(b) a cyber security incident in respect of any computer or computer system under the controller's control that is interconnected or communicates with critical information or critical information infrastructure; or

(c) any other type of cyber security incident in respect of critical information or critical information infrastructure that the Agency may specify to the controller.

(2) Despite subsection (1), a controller shall submit a preliminary cyber incident report to the Agency within twelve hours of notifying the Agency of the perceived or actual occurrence of the incident under that subsection, in a prescribed manner and form.

(3) A controller shall, as soon as the cyber security incident is resolved, submit to the Agency a detailed cyber security incident report.

(4) Despite subsection (3), a controller shall submit to the Agency a cyber security incident status report, at intervals, that the Agency may determine.

(5) A controller shall establish mechanisms and processes, in accordance with information security standards published by the Agency in the *Gazette*, for the detection of a cyber security threat in respect of critical information or critical information infrastructure.

(6) A controller who contravenes this section commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Power to investigate cyber security incident and cyber security threat

18. (1) The Agency shall, where the Agency receives information regarding an alleged cyber security threat or cyber security incident which satisfies the severity threshold in subsection (2), investigate that cyber security threat or cyber security incident, for the purposes of —

(a) assessing the impact or potential impact of the cyber security threat or incident; or

(b) preventing any or further harm arising from a cyber security threat or incident.

(2) A cyber security threat or incident satisfies the severity threshold where the cyber security threat or incident creates a risk of—

(a) significant harm being caused to critical information or critical information infrastructure; or

(b) disruption to the provision of an essential service.

(3) An inspector may, for the purpose of conducting an investigation under subsection (1) —

(a) request, by written notice, a controller to attend at a reasonable time and place as may be specified in the notice to answer any question;

(b) request, by written notice, a controller to produce a physical or electronic record, document or copy in the possession of the controller;

(c) request, by written notice, a controller to provide an inspector with information, which the inspector considers to be relevant to the investigation;

(d) copy or take extracts from any physical or electronic record or document in the possession of the controller;

(e) request for information from a person who appears to be acquainted with the facts and circumstances relating to the alleged cyber security threat or incident;

(f) direct, by written notice, a controller to carry out remedial measures, or to cease carrying on activities, as may be specified in the notice in order to minimise the cyber security threat or incident on a computer or computer system; or

(g) require the owner of a computer or computer system to take any action to assist with the investigation.

(4) An inspector may, with a warrant, where the inspector reasonably believes that there is a perceived or actual cyber security threat or incident, enter premises where a computer or computer system affected or was affected by the cyber security threat or incident is located, to —

(a) examine the operation of the computer or computer system;

(b) take a copy of, or extracts from, any electronic record or computer programme contained in a computer or computer system; or

(c) take possession of a computer or other equipment for the purpose of conducting digital forensics.

(5) The Agency shall, immediately after the completion of an examination or analysis on a computer or other equipment taken into possession by an inspector in exercise of the powers under subsection (4), return the computer or other equipment to the owner.

(6) A person commits an offence where that person willfully gives false information or without lawful excuse refuses to give information or produce a record, document or copy thereof required of that person by an inspector under this section.

(7) A person convicted of an offence under subsection (6) is liable, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year, or to both.

Cyber security exercise

19. (1) The Agency shall conduct a national cyber security exercise for the purpose of testing the state of readiness of controllers for a cyber attack at least once a year.

(2) Despite subsection (1), the Agency may conduct a cyber security exercise at intervals that the Agency may determine.

(3) A controller shall participate in a cyber security exercise as directed, in writing, by the Agency.

(4) A controller who fails to comply with a written direction issued under subsection (3) commits an offence and is liable, on conviction, to a fine not exceeding three million penalty units.

Cyber Security Risk Register

20. The Agency shall keep and maintain an electronic Cyber Security Risk Register which shall contain the following information:

(a) data of critical information or critical information infrastructure;

(b) identified and potential risks;

(c) the level of impact of risk; and

(d) any other information that the Agency may determine.

PART V

Interception Of Communications

Central Monitoring and Coordination Centre

21. (1) The Central Monitoring and Coordination Centre established under the repealed Act is continued as if established under this Act.

(2) Subject to the provisions of this Act, the Centre shall be the sole facility through which —

(a) lawful interceptions shall be effected; and

(b) intercepted communication and call related information of an interception target shall be forwarded.

(3) The Centre shall be managed, controlled and operated by the division responsible for Government communications.

Prohibition of interception of communication

22. (1) A person shall not knowingly and without lawful authority—

(a) intercept, attempt to intercept or procure another person to intercept or attempt to intercept any communication; or

(b) use, attempt to use or procure another person to use or attempt to use any electronic, software, mechanical or other device to intercept a communication.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

Prohibition of use, manufacture or possession of interception device

23. (1) A person shall not use, manufacture or possess an interception device without authorisation.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

(3) Subsection (1) does not apply to the use or possession of an interception device by an electronic communications service provider, the Agency, Authority or any other person authorised by the division responsible for Government communications, where that interception device is used—

(a) for the operation, maintenance and testing of an electronic communications service;

(b) to protect the rights or property of the electronic communications service provider or the users of the electronic communications service from abuse of that service or any other unlawful use of the service;

(c) to record that a communication was initiated or completed in order to protect —

(i) an electronic communications service provider in the completion of a communication; or

(ii) a user of an electronic communications service from fraudulent, unlawful or abusive use of that electronic communications service;

(d) pursuant to an interception of communication order; or

(e) for research purposes where consent of a user of the electronic communications service has been obtained.

(4) Despite subsection (3), an institution or person referred to under that subsection shall keep a record of the interception conducted by that institution or person using an interception device registered under section 24 and submit a copy of the record to the Centre.

(5) A person who contravenes subsection (4) commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(6) In this section, unless the context otherwise requires, "interception device" means a device designed or modified to intercept cellular communications, manipulate cellular network protocols, intercept satellite communications, intercept radio communications or capture mobile device identifiers.

Registration of interception device

24. (1) A person authorised to use or possess an interception device under section 23 shall apply to the Centre for the registration of the interception device in a prescribed manner and form on payment of a prescribed fee.

(2) The Centre shall, within fourteen days of receipt of the application under subsection (1), grant or reject the application.

(3) The Centre shall, where the Centre —

(a) grants the application under subsection (2), issue the applicant with a certificate of registration in a prescribed manner and form on terms and conditions that the Centre may determine; or

(b) rejects the application under subsection (2), inform the applicant in writing, stating the reasons for the rejection.

(4) A certificate of registration granted under subsection (3) shall be valid for a period as prescribed.

(5) A person who intends to renew a certificate of registration may, not less than three months before the expiry of the certificate of registration, apply to the Centre for renewal of the certificate of registration in the prescribed manner and form on payment of the prescribed fee.

Variation of certificate of registration

25. A holder of a certificate of registration may, at any time during the validity of the certificate of registration, apply to the Centre for a variation of the certificate of registration, in a prescribed manner and form, on payment of a prescribed fee.

Surrender of certificate of registration

26. (1) The holder of a certificate of registration shall, where the holder of a certificate of registration does not intend to continue using or possessing an interception device for the purpose to which the certificate of registration relates, surrender the certificate of registration to the Centre.

(2) Where a certificate of registration has been surrendered under subsection (1), the holder of a certificate of registration shall surrender the interception device to the Centre.

(3) The Centre shall determine the manner in which an interception device surrendered under subsection (2) shall be disposed of.

Transfer of certificate of registration

27. A certificate of registration issued under this Part shall not be transferred to a third party.

Cancellation or suspension of certificate of registration

28. (1) The Centre shall suspend or cancel a certificate of registration if a holder of the certificate of registration —

(a) obtained the certificate of registration through fraud, misrepresentation or concealment of a material fact; or

(b) contravenes any provision of this Act or terms and conditions of the certificate of registration.

(2) The Centre shall, before suspending or cancelling the certificate of registration in accordance with subsection (1), notify the holder of the certificate of registration of the Centre's intention to suspend or cancel the certificate of registration and shall —

(a) give reasons for the intended suspension or cancellation; and

(b) require the holder of a certificate of registration to show cause, within a period of not more than thirty days, why the certificate of registration should not be suspended or cancelled.

(3) The Centre shall, in making the Centre's final determination on the suspension or cancellation of a certifcate of registration, consider the submissions made by the holder of a certificate of registration under subsection (2) *(b)*.

(4) The Centre shall not suspend or cancel a certificate of registration under this section if the holder of a certificate of registration takes remedial measures to the satisfaction of the Centre within the preiond specified unders subsection (2) *(b)*.

(5) The Centre may suspend or cancel a certificate of registration if the holder of a certificate of registration after being notified under subsection (2) fails to show cause or does not take any remedial measures, to the satisfaction of the Centre, within the time specified in that subsection.

(6) The holder of a certificate of registration shall, where a certificate of registration is cancelled in accordance with subsection (5), surrender the certificate of registration to the Centre.

Lawful interception

29. (1) Subject to subsection (2), a law enforcement officer shall, where the law enforcement officer has reasonable grounds to believe that an offence has been committed, is likely to be committed, or is being committed, apply *ex-parte* to a judge for an interception of communication order.

(2) A judge to whom an application is made under subsection (1) may issue an interception of communication order—

(a) requiring an electronic communications service provider to intercept and retain specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that electronic communications service provider;

(b) authorising the law enforcement officer, through the Centre, to enter specified premises and to install on such premises any device for the interception and retention of communication or communications of a specified description and to remove and retain such device;

(c) requiring any person to furnish the law enforcement officer with information, facilities and assistance as the judge considers necessary for the purpose of the installation of the interception device; or

(d) imposing terms and conditions for the protection of interests of persons specified in the interception of communication order or any third parties or to facilitate investigations.

(3) A judge may grant an order under subsection (2), where the judge is satisfied that there are reasonable grounds to believe that the communication relates to the —

(a) commission of an offence under this Act or any other written law; or

(b) whereabouts of a person suspected by a law enforcement officer to have committed an offence is contained in that communication.

(4) An order referred to under subsection (2), shall be valid for a period of three months and may, on application by a law enforcement officer, be renewed for a further period not exceeding three months.

(5) A law enforcement officer shall on receipt of an order under subsection (2), serve the order on an electronic communications service provider.

(6) An electronic communications service provider shall, within twenty four hours of receipt of an order issued under subsection (2), route duplicate signals of an indirect communication to the Centre.

(7) The Centre shall make available to a law enforcement officer the duplicate signals of an indirect communication routed to the Centre under subsection (6).

(8) Information shall be admissible in proceedings for an offence under this Act, as evidence of the truth where that information is contained in a communication that is intercepted and retained —

(a) pursuant to an interception of communication order under subsection (2); or

(b) in a foreign State in accordance with the law of that foreign State and certified by a judge of that foreign State to have been so intercepted and retained.

(9) An action shall not lie in any court against an electronic communications service provider, any officer, employee or agent of the electronic communications service provider, for providing information, facilities or assistance in accordance with the terms of an interception of communication order under subsection (2).

Interception of communication to prevent bodily harm, loss of life or damage to property

30. (1) A law enforcement officer may orally request an electronic communications service provider to intercept any communication and to route the duplicate signals of the indirect communication specified in that request to the Centre where the law enforcement officer has reasonable grounds to believe that—

(a) a person who is party to any communication —

(i) has caused, or may cause, the infliction of bodily harm to another person;

(ii) threatens, or has threatened, to cause the infliction of bodily harm to another person;

(iii) threatens, or has threatened, to kill oneself or another person, or to perform an act which may endanger that person's own life or that of another person;

(iv) has caused or may cause damage to property; or

(v) has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries;

(b) it is not reasonably practical to make an application under section 29 for an interception of communication order as the delay to intercept a specified communication would result in the infliction of bodily harm, the death of another person or damage to property; or

(c) the sole purpose of the interception is to prevent bodily harm to, or loss of life of, any person or damage to property.

(2) An electronic communications service provider shall, on receipt of a request made under subsection (1) by a law enforcement officer, route the duplicate signals of the indirect communication to the Centre.

(3) A law enforcement officer who makes a request to an electronic communications service provider under subsection (1) shall, within twenty-four hours after making that request, furnish the electronic communications service provider with a written confirmation of the request setting out the information given by that law enforcement officer.

(4) A law enforcement officer who makes a request for interception under subsection (1), shall within two days, after the interception of the communication, submit to a judge —

(a) a copy of the written confirmation referred to in subsection (3);

(b) an affidavit setting out the results and information obtained from that interception;

(c) a recording of the communication that has been obtained through that interception; and

(d) a full or partial transcript of the recording of the communication and any notes made by the law enforcement officer.

(5) An electronic communications service provider who, in accordance with subsection (2), routes duplicate signals of indirect communications to the Centre shall, as soon as practicable, submit an affidavit to a judge setting out the steps taken by that electronic communications service provider in giving effect to the request and the results obtained from such steps.

(6) A judge may make an order as the judge considers appropriate in relation to the electronic communications service provider, the person whose communication has been intercepted or the law enforcement officer, where a judge, on receipt of a written confirmation and affidavit under this section, determines that the interception was effected or used for purposes contrary to, or in contravention of, the provisions of this Act or any other law.

Prohibition of use, acquisition, etc of geolocation and interception information

31. (1) Subject to the provisions of this Part, a person shall not, intentionally and without consent of the owner of the geolocation information, use an electronic, mechanical or other device to —

(a) acquire or attempt to acquire, geolocation information relating to another person; or

(b) disclose, or attempt to disclose or intercept communication or geolocation information relating to another person.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

(3) In this section, unless the context otherwise requires, "consent" has the meaning assigned to the word in the Data Protection Act, 2021.

Act No. 3 of 2021

Interception of communication for purposes of determining location

32. (1) Where a person is a party to a communication and that person, as a result of information received from the other party to the communication, has reasonable grounds to believe that an emergency exists and the location of that other party is unknown, that person shall, if that person is —

(a) a law enforcement officer, and has reasonable grounds to believe that determination of the location of the other party is likely to be of assistance in dealing with the emergency, request an electronic communications service provider to —

(i) intercept that communication for purposes of determining that other party's location; or

(ii) determine the location of the sender; or

(b) not a law enforcement officer, inform any law enforcement officer of the emergency.

(2) Subject to this Part, the provisions relating to interception of communication under section 29 shall apply to the interception of communication for purposes of determining geolocation with necessary modifications.

(3) An emergency for purposes of this section exists if—

(a) there is potential or actual threat to national security;

(b) there is potential or actual threat to public safety;

(c) the life of another person is likely to be endangered or is endangered; or

(d) property is likely to be damaged, is being damaged or has been damaged.

Technical assistance for purposes of determining location or illegal use of spectrum

33. (1) The Centre may, on request by a law enforcement officer, with a warrant, assist the law enforcement officer for purposes of determining a location or the location of a prohibited device as prescribed.

(2) The Authority may intercept communication for purposes of determining the location of illegal use of the spectrum or numbering resources.

Prohibition of access and use of intercepted communication

34. (1) An electronic communications service provider who intercepts a communication pursuant to an interception of communication order shall not use the communication in any manner other than in accordance with the provisions of this Act.

(2) A person commits an offence if that person without authorisation —

(a) accesses the contents of any intercepted communication; or

(b) uses, or attempts to use, the contents of any intercepted communication.

(3) A person who contravenes subsection (2), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

Disclosure of intercepted communication by law enforcement officer

35. (1) A law enforcement officer who obtains information pursuant to an interception of communication order may disclose the communication to another law enforcement officer where the disclosure is necessary for the determination of the commission of an offence or the whereabouts of a person suspected to have committed an offence.

(2) Where a law enforcement officer, in the performance of any functions under this Act, obtains information pursuant to an interception of communications order relating to the commission of an offence under any other law, the law enforcement officer shall disclose or use the communication in accordance with the provisions of this Act or that other law.

Privileged communication to retain privileged character

36. A privileged communication intercepted in accordance with the provisions of this Act shall not lose its privileged character.

Prohibition of random monitoring

37. (1) A person shall not use an electronic communications service, critical information or critical information infrastructure to randomly monitor a communication, except for mechanical or service quality control checks.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units, or to imprisonment for a term not exceeding ten years, or to both.

(3) In this section, unless the context otherwise requires —

"monitor" includes listening to, viewing, reading or recording communication by means of a monitoring device; and

"monitoring device" means any electronic, software, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to, view, read or record any communication.

Interception of satellite transmission

38. (1) An interception of satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of transmission to the public, or as an audio subcarrier intended for redistribution to facilities open to the public, is not an offence under this part unless the interception is for the purpose of a direct or indirect commercial advantage or private financial gain.

(2) Subsection (1) does not apply to a two-way data transmission or a telephone call.

Assistance by electronic communications service provider

39. (1) An electronic communications service provider shall —

(a) use an electronic communication system that is technically capable of supporting interception in accordance with this Act;

(b) install hardware and software facilities and devices to enable interception of communications when required by a law enforcement officer or under a court order;

(c) provide services that are capable of rendering real time and full time monitoring facilities for interception of communications;

(d) provide all call-related information in real time or as soon as possible on call termination;

(e) provide one or more interfaces from which an intercepted communication shall be transmitted to the Centre;

(f) transmit intercepted communication to the Centre through fixed or switched connections; and

(g) provide access to all intercepted subjects operating temporarily or permanently within the service provider's communications systems, and where the interception subject is using features to divert calls to other service providers or terminal equipment, access to such other service providers or equipment.

(2) An electronic communications service provider who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding ten million penalty units.

Interception capability of electronic communications service provider

40. (1) Despite any other written law, an electronic communications service provider shall —

(a) provide a service which has the capability to be intercepted; and

(b) store call-related information or internet connection records in accordance with the provisions of this Act.

(2) The President may, in consultation with the Centre, by statutory instrument, make Regulations to provide for the —

(a) manner in which interception capability is to be provided by an electronic communications service provider;

(b) security, technical and functional features of facilities and devices to be acquired by an electronic communications service provider to enable the —

(i) interception of communication under this Act; and

(ii) storing of call-related information and internet connection records; and

(c) period within which requirements under paragraphs *(a)* and *(b)* shall be complied with.

(3) The Regulations made under subsection (2) shall specify—

(a) the capacity and technical features of the devices or systems to be used for interception purposes;

(b) the connectivity of devices or systems to be used for interception purposes with the Centre;

(c) the manner of routing an indirect communication to the Centre; and

(d) any other matter which is necessary for the better carrying out of the provisions of this Part.

(4) An electronic communications service provider shall acquire facilities and devices specified in the Regulations made under subsection (2) at the electronic communications service provider's own expense.

(5) Subject to this Act, a cost incurred by an electronic communications service provider shall be borne by the electronic communications service provider for the purpose of —

(a) enabling —

(i) an electronic communication to be intercepted; and

(ii) call-related information to be stored; or

(b) complying with this Part.

PART VI

Licensing of Cyber Security Service Providers

Cyber security services

41. For the purposes of this Act, the following are cyber security services:

(a) penetration testing;

(b) security operations centre;

(c) information security risk assessment;

(d) vulnerability assessment;

(e) incident response;

(f) cyber audit;

(g) red teaming; or

(h) any other services as may be prescribed.

Prohibition of providing cyber security service without licence

42. (1) A person shall not provide a cyber security service without a licence issued under this Act.

(2) A controller shall not engage a person who is not licensed under this Act.

(3) A person who contravenes subsection (1) or

(2) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Categories of licences

43. There shall be categories of licences as may be prescribed for purposes of providing cyber security services specified under section 41.

Application for licence

44. (1) A person who intends to provide a cyber security service shall apply to the Agency for a licence in the prescribed manner and form on payment of a prescribed fee.

(2) The Agency shall, within thirty days of receipt of an application under subsection (1), approve or reject the application.

(3) Where the Agency fails to make a decision within the period referred to under subsection (2), the application shall be deemed to have been granted.

(4) The Agency may request for further particulars or information in respect of an application under this section in the prescribed manner and form.

Grant of licence

45. (1) The Agency shall, where the Agency approves an application under section 44, issue the applicant with a licence in a prescribed manner and form.

(2) A licence issued under this section may be issued on terms and conditions that the Agency may determine.

Rejection of application

46. (1) The Agency shall reject an application for a licence as a cyber security service provider if —

(a) an applicant or an officer of an applicant is not a fit and proper person;

(b) it is not in the public interest to grant the application;

(c) the grant of the licence may pose a threat to national security; or

(d) the applicant has not met the criteria for licensing as prescribed.

(2) The Agency shall, where the Agency rejects an application for a licence on the grounds set out in subsection (1), inform the applicant, in writing, stating the reasons for the rejection.

(3) For the purposes of subsection (1), an applicant or an officer of the applicant is not a fit and proper person, if that applicant or officer—

(a) is legally disqualified;

(b) is an undischarged bankrupt;

(c) has been convicted of an offence involving fraud or dishonesty;

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

(e) does not meet any other criteria that may be determined by the Agency.

(4) In this section, unless the context otherwise requires, "officer" means a director, a partner of the applicant or any person who is responsible for conducting cyber security services.

Variation of licence

47. A holder of a licence may, at any time during the validity of the licence, apply to the Agency for a variation of the licence in a prescribed manner and form on payment of a prescribed fee.

Surrender of licence

48. The holder of a licence shall, where the holder of a licence does not intend to continue operating as a cyber security service provider to which the licence relates, surrender the licence to the Agency.

Transfer of licence

49. A licence issued under this Part shall not be transferred to a third party.

Renewal of licence

50. (1) A cyber security service provider that intends to renew a licence shall, not less than three months before expiry of the licence, apply for renewal of the licence in the prescribed manner and form on payment of a prescribed fee.

(2) The Agency shall renew the licence if the cyber security service provider remains in compliance with the conditions of the licence under this Act.

(3) A licence renewed under this section shall be valid for a period that the Agency may determine.

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

Cancellation or suspension of licence

51. (1) The Agency shall suspend or cancel a licence if a holder of the licence —

(a) obtained the licence through fraud, misrepresentation or concealment of a material fact;

(b) is insolvent;

(c) is legally disqualified from operating a cyber security service;

(d) is convicted of an offence under this Act or any other written law and sentenced to imprisonment for a term exceeding six months without the option of a fine; or

(e) contravenes any provision of this Act or terms and conditions of the licence.

(2) The Agency shall, before suspending or cancelling the licence in accordance with subsection (1), notify the holder of the licence of the Agency's intention to suspend or cancel the licence and shall —

(a) give reasons for the intended suspension or cancellation; and

(b) require the holder to show cause, within a period of not more than thirty days, why the licence should not be suspended or cancelled.

(3) The Agency shall not suspend or cancel a licence under this section if the holder takes remedial measures to the satisfaction of the Agency within the period specified under subsection (2).

(4) The Agency shall, in making the Agency's final determination on the suspension or cancellation of a licence consider the submissions made by the holder of a licence under subsection (2).

(5) The Agency may suspend or cancel a licence if the holder after being notified under subsection (2) fails to show cause or does not take any remedial measures, to the satisfaction of the Agency, within the time specified in that subsection.

(6) The holder of a licence shall, where a licence is cancelled in accordance with subsection (5), surrender the licence to the Agency.

Register of cyber security service providers

52. The Agency shall keep and maintain a register of cyber security service providers in the prescribed manner and form.

PART VII

International Cooperation in Maintaining Cyber Security

Identifying areas of cooperation

53. Subject to section 3(3), the Agency shall identify and ensure that the Agency cooperates with private bodies, organisations and Government entities involved in cyber security matters, within and outside the Republic.

Entering into agreement

Cap. 98

54. Subject to the Mutual Legal Assistance in Criminal Matters Act, the Republic may enter into an agreement with a foreign State 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 the Republic which is or was committed by the use of an article; or

(c) an offence substantially similar to an offence recognised in the Republic which is or was committed by the use of an article, in the foreign State.

PART VIII

Inspectorate

Appointment of cyber security inspector

55. (1) The Agency shall appoint a suitably qualified person to be a cyber security inspector for the purposes of ensuring compliance with this Act.

(2) The Agency shall, issue an official identification document to an inspector, which shall be *prima facie* evidence of an inspector's appointment.

(3) An inspector shall, in performing any function under this part —

(a) be in possession of the official identification document referred to in subsection (2); and

(b) show the official identification document to a person who requests to see the official identification document.

Power to access, search and seize

56. (1) An inspector may, for the purposes of enforcing the provisions of this Act, at any reasonable time, and with a warrant —

(a) enter the licensee or controller's premises or access a computer or computer system in the private domain;

(b) monitor a computer or computer system;

(c) search any person on the licensee or controller's premises, document or record that has a bearing on an investigation, except that a person shall be searched by a person of the same sex;

(d) seize a computer or computer system that has a bearing on an investigation;

(e) take extracts from, or make copies of a book, document or record that is on or in the licensee or controller's premises or in the computer or computer system that has a bearing on an investigation;

(f) access and inspect the operation of any computer, computer system or equipment forming part of an information system and any associated apparatus or material which the inspector has reasonable cause to believe is, or has been used in, connection with any offence; and

(g) use or cause to be used any computer or computer system or part thereof to search any data contained in or available to such a computer or computer system.

(2) An inspector who removes anything from any premises shall —

(a) issue a receipt for anything removed to the owner or the person in control of the premises; and

(b) return anything removed as soon as practicable after the thing has served the purpose for which it was removed.

(3) Despite subsection (1), an inspector may without a warrant —

(a) conduct an information security audit on critical information, critical information infrastructure or an electronic communications system accessible in the public domain;

(b) require a person in control of, or involved in, the operation of a computer or computer system of a licensee or controller, to provide the inspector with reasonable technical and other assistance as the inspector may require for the purposes of this Part;

(c) demand the production of, and inspect, relevant licences and registration certificates; and

(d) inspect a computer or computer system associated with the computer or computer system of a licensee or controller.

(4) A person commits an offence if that person —

(a) delays or obstructs an inspector in the performance of that inspector's functions under this Act;

(b) refuses to give an inspector such reasonable assistance as the inspector may require for the purpose of performing the inspector's functions;

(c) impersonates an inspector or presents oneself to be an inspector; or

(d) willfully gives an inspector false or misleading information in answer to an inquiry made by the inspector.

(5) A person convicted of an offence under subsection (4) is liable, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Appointment of cyber security technical expert

57. (1) The Agency may appoint a person as a cyber security technical expert for a specified period, to assist an inspector in the inspector's exercise of any powers under this Act.

(2) The Agency shall issue an official identification document to the cyber security technical expert which shall be *prima facie* evidence of a cyber security technical expert's appointment.

(3) A cyber security technical expert shall, in performing any function under this part —

(a) be in possession of the official identification document referred to in subsection (2); and

(b) show the official identification document to a person who requests to see the official identification document.

(4) The Agency shall determine the terms and conditions of the appointment of the cyber security technical expert.

PART IX

General Provisions

Appeals

58. A person aggrieved by a decision of the Agency may, within thirty days of the decision, appeal to the High Court.

Search and seizure by law enforcement officer

59. (1) A law enforcement officer may, with a warrant, enter any premises to search and seize a computer or computer system, where a computer or computer system contains material—

(a) or evidence necessary in proving an offence; or

(b) that has been acquired by a person as a result of an offence.

(2) A law enforcement officer who is undertaking a search under this Act may, where the law enforcement officer has reasonable grounds to believe that the data sought is stored in another device, computer or computer system or part of it, and such data is lawfully accessible from or available to an initial device or system, extend the search or access to the other device or system.

Restoration of property

60. (1) A law enforcement officer shall, where a person from whom a computer or computer system has been seized under section 59 is found not guilty or the proceedings against that person are withdrawn —

(a) within thirty days of the finding of the court or the withdrawal of proceedings, restore a computer or computer system to that person; or

(b) where the law enforcement officer is satisfied that the person cannot be found or is unwilling to receive the computer or computer system, apply to the court for an order of forfeiture of the computer or computer system.

Act No. 19 of 2010

(2) Subject to the Forfeiture of Proceeds of Crimes Act, 2010, the court shall make an order of forfeiture under subsection (1) if —

(a) the law enforcement officer has given notice, by publication in the *Gazette* and in a daily newspaper of general circulation in the Republic, to the effect that the computer or computer system which has been seized under this Act shall vest in the State if it is not claimed within three months from the date of publication of the notice; and

(b) three months after the giving of the notice under paragraph *(a),* the computer or computer system remains unclaimed.

(3) Where a claim is made, in writing, by a person that is lawfully entitled to the computer or computer system seized under this Part, the law enforcement officer may order the release of the computer or computer system to the claimant if satisfied that there is no dispute concerning the ownership of the computer or computer system and that it is not liable to forfeiture.

Assistance

61. A person, who is not a suspect of a crime or otherwise excluded from an obligation to provide assistance, but who has knowledge about the functioning of a computer or computer system or measures applied to protect the computer data that is the subject of a search under this Act may, permit and assist where reasonably required and requested by a person authorised to make the search by —

(a) providing information that enables the undertaking of necessary measures in the circumstances;

(b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the computer system;

(c) obtaining and copying such computer data; or

(d) obtaining an intelligible output from a computer system in a format that is admissible for the purpose of legal proceedings.

Evidence obtained by unlawful interception not admissible in criminal proceedings

62. Despite any other law, evidence which is obtained by means of an interception effected in contravention of this Act, shall not be admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave, the court shall have regard to the circumstances in which the evidence was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused person that may be occasioned by its admission or exclusion.

Prohibition of obstruction of law enforcement officer

63. (1) A person who obstructs or hinders a law enforcement officer, in the exercise of any powers under this Act or neglects or fails to comply with a lawful order of a law enforcement officer commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Submission of information by controller

64. (1) A controller shall, annually submit to the Agency in writing, such information as the Agency may determine.

(2) A controller who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year, or to both.

General penalty

65. A person who commits an offence under this Act for which no penalty is provided for is liable, on conviction, in the case of —

(a) an individual, to a penalty not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both; or

(b) a body corporate or unincorporate body, to a penalty not exceeding one million penalty units.

Power of court to order cancellation of licence, forfeiture etc.,

66. (1) A court may, on conviction of a person of an offence under this Act order —

(a) forfeiture of —

(i) property constituting proceeds of such offence; or

(ii) device or property used or intended to be used to commit or facilitate the commission of the offence; or

(b) the cancellation of a licence issued under this Act.

Act No. 19 of 2010

(2) The Forfeiture of Proceeds of Crimes Act, 2010, applies in relation to an order of forfeiture made by the court under subsection (1).

Guidelines

67. (1) The Agency may issue guidelines as are necessary for the better carrying out of the provisions of this Act.

(2) The Agency shall publish the guidelines on the Agency's website, in a daily newspaper of general circulation in the Republic, the *Gazette* or any other electronic platform.

(3) The guidelines issued by the Agency under this Act shall bind all persons regulated under this Act and may include guidelines relating to —

(a) cyber incident reporting;

(b) cyber security;

(c) cyber resilience;

(d) critical information infrastructure risk assessments;

(e) critical information infrastructure data retention; and

(f) cyber incident management exercises.

Standards

68. The Agency may develop standards for the regulation of cyber security in the Republic.

Exemptions

69. (1) The Agency may, by notice in the *Gazette* or daily newspaper of general circulation in the Republic, exempt a person or class of persons, for a limited or unlimited period of time, from the requirement to comply with the provisions of Part IV and Part VI.

(2) The Agency may, where the Agency issues a notice under subsection (1), revoke its decision where it considers necessary to do so.

(3) The Agency may where the Agency revokes its decision under subsection (2), publish the decision by notice in the *Gazette* or a daily newspaper of general circulation in the Republic.

Compounding of certain offences by Agency

70. Subject to the written consent of the Director of Public Prosecutions and where the Agency is satisfied after an investigation, and a person admits that the person has committed an offence under this Act, the Agency may compound the offence by collecting from that person a sum of money that the Agency considers appropriate, but not exceeding fifty percent of the maximum amount of the fine to which that person would have been liable on conviction, and a person having made that payment shall not thereafter be prosecuted in relation to the offence so compounded.

Administrative penalty

71. (1) The Agency may impose an administrative penalty on a person for failure to comply with a provision of this Act which is not an offence.

(2) An administrative penalty shall not exceed the amount prescribed by the President by statutory instrument for each day during which the failure continues.

(3) An administrative penalty shall be paid to the Agency within the period prescribed by the President.

(4) The Agency may, where a person fails to pay an administrative penalty within the stipulated period under subsection (3), by way of civil action in a competent court, recover the amount of the administrative penalty from that person as an amount due and owing to the Agency.

Regulations

72. (1) The President may, on the recommendation of the Agency, by statutory instrument, make Regulations for the better carrying out of the provisions of this Act.

(2) Despite the generality of subsection (1), the regulations may make provisions for —

(a) the form and manner of making applications for registration, licences, duration of licences and the fees payable on that application;

(b) critical sectors;

(c) baseline security requirements for critical information or critical information infrastructure;

(d) manner of hosting of critical information;

(e) factors to consider for hosting of critical information outside the Republic;

(f) cyber security services;

(g) categories of licences of cyber security services; or

(h) any other matter required to be prescribed under this Act.

Repeal of Act No. 2 of 2021

73. The Cyber Security and Cyber Crimes Act, 2021 is repealed.

APPENDIX

SCHEDULE

(Section 2)

STAFF BOARD

Staff Board

1. The President shall constitute the Staff Board which shall consist of part-time members who shall advise the Director-General on the selection, appointment, termination of appointment, promotion and discipline of officers below the rank of Deputy-Director.

2. Subject to any specific or general direction of the President, the Staff Board may regulate its own procedure.

3. The President shall appoint a Chairperson of the Staff Board from amongst the members.

4. The Members of the Staff Board shall elect the Vice-Chairperson from amongst themselves.

5. The President may, by statutory instrument, make regulations to provide for the composition, allowances and tenure of the Staff Board.