ACT

THE CYBER SECURITY AND CRIME ACT, 2021

ARRANGEMENT OF SECTIONS

PART I –PRELIMINARY

Section

PART II–ADMINISTRATION AND COORDINATION

PART III–CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

PART IV–POWERS AND PROCEDURES

DR. JULIUS MAADA BIO,
President.

LS

No. **2021**

The Cyber Security and Crime Act, 2021. Short title.

Being an Act to provide for the effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes; prevention of the abusive use of computer systems; to provide for the establishment of structures to promote cybersecurity and capacity building; to provide for the timely and effective collection of electronic evidence for the purpose of investigation and prosecution of cybercrime; to provide for the protection of Critical National Information Infrastructure and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights to provide for facilitation of international cooperation in dealing with cybercrime matters and to provide for other related matters.

[ ]

ENACTED by the President and Members of Parliament in this present Parliament assembled. Date of commencement.

PART I – PRELIMINARY

Interpretation.

1. In this Act, unless the contrary intention appears -

"Attorney General" means The Attorney-General and Minister of Justice established under the Constitution;

"authorised person" means a member of the National Cyber Security Coordination Center or a person mandated by it, involv in the prohibition, prevention, elemination or combating of Computer crimes and Cyier Security threats.

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

"computer data storage medium" means any device, physical or virtual, containing or designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed form for use by a computer;

"computer system" means any physical or virtual device, or any set of associated physical or virtual devices; or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data at least one of which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system;

"crime against humanity" includes any of the following acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment, torture rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilisation or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhumane acts of similar character intentionally causing great suffering or serious bodily or mental injury;

"Critical National Information Infrastructure" means computer systems that are necessary for the continuous delivery of essential services that Sierra Leone relies on, the loss or compromise of which will lead to a debilitating impact on-

(a) the security, defence or international relations of Sierra Leone;

(b) the existence or identity of a confidential source of information relating to the enforcement of the criminal law;

(c) the provision of services directly related to communications, infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including system related to essential emergency services;

"Cyberstalking" is when a person intentionally initiate communications or a course of conduct directed at a specific person or persons with the intent to coerce, intimidate, harass, or cause emotional distress.;

"Cybersquatting" means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain is;

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"database" means digitally organized collection of data for one or more purposes which allows easy access, management and update of data;

"device" means any object or equipment that has been designed to do a particular job or whose mechanical or electrical workings are controlled or monitored by a microprocessor;

"electronic communication" means communications in electronic format, instant messages, short message

service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager;

"enforcement officer" means an officer in a law enforcement agency trained in cyber security work designated or authorised to carryout functions including for the purposes of Part IV of this Act;

"extradite" means the legal obligation of states under public international law to handover persons who commit international crimes to a foreign state for indictment, prosecution or imprisonment.

"encrypted data" means data which has been transformed from its plain text version to an unintelligible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such data occurs or can be found, for the purposes of protecting the content of such data;

"false news" means incorrect deceptive information or propaganda, misinformation or hoaxes deliberately spread under the guise of being authentic news via traditional print and broadcast news media or online social media written and published with the intent to mislead for gains;

"Financial Institution" means any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities, a discount house, finance company and money brokerage whose principal object includes factoring project financing equipment leasing, debt administration, fund management, private ledger services, investment management, local purchase order financing, export

finance, project consultancy, financial consultancy, pension fund management, insurance institutions, debt factorization and conversion firms, dealer, clearing and settlement companies, legal practitioners, hotels, casinos, bureau de change, supermarkets and such other businesses as the Central Bank or appropriate regulatory authorities may, from time to time, designate;

"Financial Transaction" means a transaction which in any way involves movement of funds by wire or other electronic means; involving one or more monetary instruments; or the transfer of title to any real or personal property;

"function" means logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to or from, or within a computer;

"genocide" means any of the following acts committed with intent to destroy in whole or in part, a national, ethnic, racial or religious group as such: killing members of the group, deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part, imposing measures intended to prevent births within the group; forcibly transferring children of the group to another group;

"identity theft" means the stealing of somebody else personal identifying information and pretends to be that person in order to commit fraud or to gain other financial benefits such as making unauthorised transactions or purchases.

"interference" means any impairment to the confidentiality, integrity or availability of a computer system, or any program or data on a computer system,

or any act in relation to a computer system which impairs the operation of the computer system, program, or data;

"law enforcement agencies" means any agency for the time being responsible for implementation and enforcement of the provisions of this Act;

"Minister" means the Minister responsible for Information and Communications;

"modification" means in relation to a computer system, program or data, the alteration or modification with respect to the contents of a computer system by the operation of a function of the computer system or any other computer if ;

(a) a program or data held in the computer system is altered or erased;

(b) a program or data is added to its contents; or

(c) an act occurs which impairs the normal operation of a computer system,

and any act which contributes towards causing such alteration or modification shall be deemed to have caused it;

"password" means any data by which a computer service or a computer system is capable of being obtained or used;

"person" includes a natural person, a corporation, company, partnership, firm, association or societies;

"Phishing" means the criminal and fraudulent process

of acquiring or attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as an authentic entity in an electronic communication through emails, telephone or text message asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user;

"plain text" means original data before it has been transformed into an unintelligible format.

"plain text version" means original data before it has been transformed into an unintelligible format.

"pornography" means the representation in books, magazines, photographs, films, and other media, telecommunication apparatus of scenes of sexual behavior that are erotic or lewd and are designed to arouse sexual interest;

"premises" means land, buildings, movable structures, a physical or virtual space in which data is maintained, managed, backed up remotely and made available to users over a network, vehicles, vessels or aircraft;

"President" means the President of the Republic of Sierra Leone as established by the Constitution.

"program or computer program" means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"prosecute" means the legal obligation of states under public international law to prosecute persons who commit international crimes where no other state has requested extradition;

"racist or xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

"Requested State" means a state being requested to provide legal assistance under the terms of this Act;

"Requesting State" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Sierra Leone is obligated;

"service provider" means a public or private entity that provides to users of its services the means to communicate by use of a computer system including any other entity that processes or stores computer data on behalf of that entity or its users;

"seize" with respect to a program or data be defined to include:

(a) secure a computer system or part of it or a device;

(b) make and retain a digital image or secure a copy of any program or data, including using an on-site equipment;

(c) render the computer system inaccessible;

(d) remove data in the accessed computer system; or

(e) obtain output of data from a computer system;

"Sexually explicit conduct" includes at least the following real or simulated acts done with intent to exploit a child-

(a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, involving a child, or between an adult and a child, of the same or opposite sex;

(b) bestiality;

(c) masturbation;

(d) sadistic or masochistic abuse in a sexual context; or

(e) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated;

"Spamming" means deliberate abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations;

"subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established-

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal, geographic, electronic mail address, telephone and other

access number, billing and payment information available on the basis of a service agreement or arrangement; or

(c) any other information on the site of an installation of communication equipment available on the basis of a service agreement or arrangement;

"traffic data" means computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or the type of underlying service;

"unauthorised" means access of any kind, to a computer system, program or data, by a person who-

(a) is not entitled to access that computer system, program or data; and

(b) does not have or exceeds the level of authorisation consented to by the person entitled to grant such consent, for the particular kind or type of access with respect to that computer system, program or data:

Provided that any act or access in exercise of powers under this Act shall not be deemed to be unauthorised.

PART II ADMINISTRATION AND COORDINATION

Establishment of the National Computer Security Incidence Response Coordination Centre

2. (1) There is established a National Computer Security Incidence Response Coordination Centre responsible for managing cyber security incindences in Sierra Leone, headed by the National Cyber Security Coordinator, who subject to the approval of Parliament shall be appointed by the President on the recommendation of the Minister

(2) The National Cybersecurity Coordinator shall hold office for a term of (5) years and is eligible for reappointment for another term of (5) years only.

(3) A person shall not be appointed National Cyber Security Coordinator unless that person has relavant knowledge, qualification and expertise in either Computer Science, Information Technology, Cyber Security or Information Security and related matters of at least (10) years and is a person of proven integrity.

(4) The National Cybersecurity Coordinator shall cease to hold office on any of the following grounds:

(a) for his or her inability to perform the functions of the office by reason of infirmity of mind or body;

(b) for proven misconduct;

(c) if he becomes bankrupt or insolvent;

(d) if he is convicted and sentenced for an offence involving fraud or dishonesty;

(e) if he resigns his office by written notice to the minister; or

(f) at the expiration of his term of office.

Functions and Powers of the Center.

3. The National Computer Security Incidence Response Coordination Center shall be responsible for cyber security issues under this Act including:

(a) provision of support to computer systems and networks in preventing and combating cybercrime in Sierra Leone;

(b) formulation and implementation of national cyber security policy and cyber security strategy;

(c) overseeing of the management of computer forensic laboratories;

(d) provision of support to the Judiciary and other law enforcement agencies in the discharge of their functions in relation to cybercrime in Sierra Leone;

(e) promotion of Sierra Leone's involvement in international cyber security cooperation; and

(f) doing such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.

Establishment of the National Cybersecurity Advisory Council.

4. (1) There is established, a National Cybersecurity Advisory Council comprising the Vice President as Chairman and the following other members-

(a) the Minister of Finance;

(b) the Attorney-General and Minister of Justice;

(c) the Minister of Internal Affairs;

(d) the Minister of Foreign Affairs and International Cooperation;

(e) the National Security Coordinator, Office of National Security;

(f) the Director-General, Central Intelligence and Security Unit;

(g) the Chief of Defence Staff, Republic of Sierra Leone Armed Forces;

(h) the Inspector-General, Sierra Leone Police;

(i) the Director-General, National Telecommunications Commission;

(j) the Governor, Bank of Sierra Leone;

(k) the National Cyber Security Coordinator as Secretary

(l) the Director General Financial Intelligence Unit

(m) the Minister of Information and Communications.

(n) a barrister and solicitor of over 15 years post enrolment at the bar nominated by the Sierra Leone Bar Association, appointed by the President.

(2) A member of the Council shall cease to hold office if-

(a) he ceases to hold the office on the basis of which he became a member of the Council; or

(b) the member listed in paragraph (n) of clause 4 (1) shall cease to hold office only for stated misconduct or infirmity of body or mind for a term of 3 years which said term may where the President deems fit be renewed for a further term of 3 years without any further renewal.

(3) The meeting of the Council shall be presided over by the Vice President and the Council shall meet, at least, 4 times a year.

Functions and Powers of the Council.

5. (1) The Council shall-

(a) provide strategic leadership, oversight and guidance on implementation and development of national cyber security legal framework in Sierra Leone in order to ensure that-

(i) Sierra Leone's cybercrime policies and laws are in conformity with regional and international standards;

(ii) there is maintenance of international cooperation required for preventing and combating cybercrimes and promoting cybersecurity; and

(iii) effective prosecution of cybercrimes and cyber security matters.

(b) make recommendation to Government on issues relating to the prevention and combating of cybercrime and the promotion of cyber security in Sierra Leone;

(c) provide general policy guidelines for the implementation of this Act; and

(d) promote the development of educational programs and research in cyber security defences, techniques and processes.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such others matters as Council may from time to time determine.

Establishment of National Cybersecurity Fund.

6. (1) There is established a fund which shall be known as the National Cyber Security Fund.

(2) There shall be paid and credited into the Fund established under subsection (1) and domiciled in the Central Bank of Sierra Leone -

(a) grants-in-aid and assistance from donor, bilateral and multilateral agencies;

(b) all other sums accruing to the Fund by way of gifts, endowments, bequests or other voluntary contributions by persons and organisations:

Provided that the terms and conditions attached to such gifts, endowments, bequests or contributions will not jeopardize the functions of the Council; and

(c) allocation from the consolidated fund;

(d) all other monies or assets that may, from time to time accrue to the Fund.

(3) An amount not exceeding 30 percent of the Fund may be allocated for programs relating to public education and awareness raising on cyber security issues.

(4) (i) The office of the National Computer Security Incidence Response Coordination Centre shall keep proper records of the accounts in a form approved by the Auditor General.

(ii) The books of account kept under sub-section (4) (i) shall within 3 months after the end of each financial year be audited by the Auditor General or an auditor appointed by him.

(iii) The financial year shall be the same as the financial year of the Government.

(5) (i) The Council shall, as soon as possible but not later than 6 months after the end of each financial year, submit to the Minister a report of the activities, operations, undertakings, properties and financies of the National Computer Security Incidence Response Coordination Center for that year, including the Auditor General's Report.

(ii) The Minister shall within 30 days of the receipt of the report referred to in sub-section (5)(i) lay a copy before Parliament.

PART III-CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Designation Of Critical National Information Infrastructure.

7. (1) The Minister shall in consultation with the National Cybersecurity Council recommend to the President who may by Order published in the Gazette, designate certain computer systems, computer data or traffic data vital to Sierra Leone or any combination of those matters, as constituting Critical National Information Infrastructure.

(2) A Presidential Order made under subsection (1), shall prescribe minimum standards, guidelines, rules or procedures reasonably required in respect of-

(a) the protection or preservation of Critical National Information Infrastructure;

(b) the general management of Critical National Information Infrastructure;

(c) the implementation of critical information systems to ensure all systems are secured by default and system and user activities are logged to facilitate accurate and efficient information systems operations audits.

(d) access to, transfer and control of data in Critical National Information Infrastructure;

(e) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated Critical National Information Infrastructure;

(f) the storage or archiving of data or information designated as Critical National Information Infrastructure;

(g) recovery plans in the event of disaster, breach or loss of the Critical National Information Infrastructure or any part of it; and

(h) any other matter required for the adequate protection, management and control of data and other resources in any Critical National Information Infrastructure.

(i) respect for and protection of the fundamental freedoms, including the right to privacy.

Audit and Inspection of Critical National Information Infrastructure.

8. A Presidential Order made under subsection (1) of section 7 may require the National Computer Security Incidence Response Team established under section (2) to audit and inspect any Critical National Information Infrastructure at any time to ensure compliance with the provisions of this Act.

PART IV - POWERS AND PROCEDURES

Scope of Powers and Procedures.

9. (1) Powers and procedures under this Act shall be applicable to and may be exercised with respect to-

(a) criminal offences under this Act;

(b) criminal offences committed by means of a computer system, including mobile phones and other electronic equipment, under any other law; and

(c) the collection of evidence in electronic form of a criminal offence under this Act or any other law.

(2) In a trial of an offence under any law, the fact that evidence has been generated, transmitted or seized from or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted provided that the evidence has been properly obtained and preserved.

(3) The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under the Criminal Procedure Act, when exercised lawfully by any other law enforcement agency or service or any regulatory authority that by itself does not investigate or prosecute an offence.

Search and Seizure of Stored Computer data.

10. (1) Upon an application by an enforcement officer or other authorised person to a Judge of the High Court that there is reasonable grounds to believe that there may be in a specified computer system, program, data, computer data storage medium material specifying the basis of the belief and the scope of the warrant required which-

(a) may be reasonably required as evidence in proving a specifically identified offence in a criminal investigation or criminal proceedings;

(b) has been acquired by a person as a result of the commission of an offence,

the Judge may issue a warrant which shall authorise the enforcement officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.

(2) A warrant issued under subsection (1) shall authorize an enforcement officer or other authorised person to-

(a) enter and search any premises or place if within those premises or place-

(i) an offence under this Act is being committed; or

(ii) there is evidence of the commission of an offence under this Act; or

(iii) there is an urgent need to prevent the commission of an offence under this Act

(b) search any person found on any premises or place which such authorised officers who are empowered to enter and search under paragraph (a) of subsection 1;

(c) stop, board and search where there is evidence of the commission of an offence under this Act;

(d) seize or secure a computer system or part of it or a computer-data storage medium;

(e) make and retain a copy of computer data;

(f) maintain the integrity of stored computer data;

(g) render inaccessible or remove computer data in the accessed computer system;

(h) have access to, inspect and check the operation of a computer system to which the warrant applies;

(i) have access to any information, obtained from the encrypted data contained or available to

a computer system into an intelligible format for the purposes of the warrant;

(j) require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer data therein, to provide the necessary computer data or information, to enable an enforcement officer or other authorised person in conducting an activity authorised under this section;

(k) have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.

(l) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

(3) An application under subsection (1) shall provide reasons explaining why it is believed that-

(a) the material sought will be found on the premises to be searched; or

(b) the purpose of an investigation search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.

(4) The court may issue a warrant under subsection (2) of this section where it is satisfied that-

(a) the warrant is sought to prevent the commission of an offence under this Act or

to prevent the interference with investigative process under this Act; or

(b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or

(c) there are reasons for believing that the person or material on the premises may be relevant to the cyber crime or computer related offences under investigation; or

(d) there are reasons to believe that the person named in the warrant is preparing to commit an offence under this Act.

Provided that any such warrant is issued access shall be without prejudice to the rights to privacy of persons and may be rescinded upon an application by a person affected to a Judge of the High Court.

(5) Where an enforcement officer or other authorised person (s) authorised to search or access a specific computer system or part of it has reasonable grounds to believe that the data sought is stored in another cloud computer system and there is reasonable grounds to believe that such data is accessible from or available to the initial system, the enforcement officer or other authorised person may extend the search or accessing to such other system or systems.

(6) Computer data seized under subsection (2) shall only be lawfully used for the purpose for which it was originally obtained.

(7) An enforcement officer or other authorised person shall-

(a) only seize a computer system under sub-section (2) when it is-

(i) not practical to secure the computer data; or

(ii) necessary to ensure that data will not be destroyed, altered or otherwise interfered with;

(b) exercise reasonable care while the computer system or computer data storage medium is retained.

(8) An enforcement officer or other authorised person who intentionally, recklessly or negligently misuses the powers granted under this section commits an offence and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not more than 5 years or to both such fine and imprisonment.

(9) A person who willfully obstructs an enforcement officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to a fine not less than Le5,000,000 and not more than Le30,000,000 or to a term of imprisonment not less than 6 months and not more than 3 years or to both such fine and imprisonment and in the case of a corporation, partnership or association to a fine not less than Le 50,000,000 and not more than Le100,000,000.

Record of and Access to Seized Data.

11. (1) Where a computer system or data has been removed or rendered inaccessible, following a search or seizure, the person who made the search or seizure shall, at the time of the search or seizure or as soon as practicable after the search -

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to -

(i) the occupier of the premises; or

(ii) the person in control of the computer system.

(2) Subject to subsection (3), an enforcement officer or other authorised person shall, on request, permit a person-

(a) who has custody or control of a computer system,

(b) who has right to data or information seized under subsection (2) of section 10; or

(c) acting on behalf of a person under subparagraph (a) or (b),

to access and copy computer data on the system or give such person a copy of the computer data.

(3) An enforcement officer or other authorised person may refuse to give access or provide copies seized under subsection (2) if he has reasonable grounds to believe that giving access or providing copies would-

(a) constitute a criminal offence; or

(b) prejudice-

(i) an investigation; or

(ii) any prosecution:

(4) Notwithstanding subsection (3), a Judge of the High Court may, upon sufficient and reasonable grounds, allow a person under sub paragraph (a), (b) or (c) to access or copy computer data.

(5) The National Computer Security Incidence Response Team shall develop standards, policies, procedures and guidelines to be used in the implementation of this Act subject to the approval of the National Cyber Security Advisory Council in respect of:

(a) the warrant request process;

(b) the process of collecting and handling evidence;

(c) chain of custody of evidence collected;

(d) processes related to device collection;

(e) processes related to email collection;

(f) the storage and inventory of data or evidence collected;

(g) the process of examining evidence;

(h) the analysis of data and evidence collected; and

(i) evidence reporting.

Production Order.

12. (1) Where it is necessary or desirable for the purposes of an investigation under this Act, a Judge of the High Court may upon an application by an enforcement officer or other authorised person, order-

(a) a person in possession or control of specified data stored in a computer system or a computer data storage medium; or

(b) a service provider in possession or control of specified subscriber information relating to services offered -

(i) in Sierra Leone; or

(ii) based outside Sierra Leone but, offering its services in Sierra Leone;

to submit information in his possession or control.

(2) A Judge of the High Court may, by order, require a person-

(a) to whom an order is made under subsection (1), or

(b) in control of a computer system, to whom a warrant is issued under subsection (1) of section 10;

to keep such order or warrant confidential.

(3) A person who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 5,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 6 months and not more than 3 years or to both such fine and imprisonment and for a corporation partnership or association not less than Le100, 000,000 and not more than Le250, 000,000.

(4) An enforcement officer or other authorised person who uses the powers granted under subsection (1) for a purpose other than that stated in section 10 commits an offence and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not more than 5 years or to both such fine and imprisonment.

(5) An application under subsection (1) shall state the reasons explaining why it is believed that-

(a) a specified computer data sought is likely to be available with a person mentioned in subparagraph (a) or (b) of subsection (1);

(b) an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;

(c) the type of evidence suspected is likely to be produced by a person mentioned in subparagraph (a) or (b) of subsection (1);

(d) subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data;

(e) an identified offence is an offence in respect of which the order is sought;

(f) measures taken shall prepare and ensure that the specified computer data will be produced-

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party who is not part of the investigation; and

(g) measures taken shall prepare and ensure that the production of the specified computer data is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.

(6) Notwithstanding the provision of sub-section (1) above, a service provider or a person in possession or control of relevant specified data shall have the right to apply to the Judge of the High Court to challenge the issuance of a production order issued under this section on the ground of relevance, privilege, capacity to implement provisions of the order or otherwise protected from disclosure by law, or non-satisfaction of the requirements in sub-section (5) of this Section.

Expedited Preservation and Partial Disclosure of Traffic Data.

13. (1) An enforcement officer or other authorised person may, where he is satisfied that-

(a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible,

by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expeditious preservation of the computer data.

(2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify-

(a) the service providers; and

(b) the path through which the communication was transmitted.

(3) The period of preservation of data required under subsection (1) shall be for a period not exceeding 30 days.

(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by an enforcement officer or other authorised person, where such extension is reasonably required for the purposes of-

(a) an investigation or prosecution;

(b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or

(c) averting overly burdensome cost of such preservation on the person in control of the computer system.

(5) A person to whom a notice under subsection (1) is given shall-

(a) be responsible to preserve the data for -

(i) a period not exceeding 30 days as specified in subsection (3); or

(ii) any extended period permitted by a Judge of the High Court under subsection (4).

(b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests, and

(c) disclose as soon as practicable, a sufficient amount of the non-content data to enable an enforcement officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication.

Real-Time Collection of traffic Data.

14. (1) Where there are reasonable grounds to believe that traffic data associated with specified communications is reasonably required for the purposes of a specific criminal investigation, a Judge of the High Court may, on an application by an enforcement officer or other authorised person, order a service provider with the capacity to monitor, collect and record to-

(a) collect or record traffic data in real-time; and

(b) provide specified traffic data to an enforcement officer or other authorised person.

(2) An Order for the real-time collection or recording of traffic data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event for not more than 30 days.

(3) A period of real-time collection or recording of traffic data under subsection (2) may be extended by a Judge of the High Court for a further reasonable specified period of time the same to be for an additional period of 30 days, on an application by an enforcement officer or other authorised person, where the extension is reasonably required for the purposes of-

(a) an investigation or prosecution;

(b) further real-time collection or recording of traffic data necessary to achieve the purpose for which the Order under sub-section (1) was made;

(c) ensuring that the real-time collection or recording of traffic data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;

(d) preventing the investigation of being frustrated or seriously prejudiced; and

(e) averting overly burdensome cost of such extension on the person in control of the computer system.

(4) An application under subsection (1) shall state reasons explaining why it is believed that-

(a) a traffic data sought will be available with the person in control of the computer system;

(b) a type of traffic data suspected will be found on that computer system;

(c) the subject of an investigation or prosecution may be found on that computer system;

(d) an identified offence is an offence in respect of which the order is sought;

(e) measures shall be taken to maintain the privacy of other users, customers and third parties; and

(f) there will be no disclosure of data of any party not part of the investigation.

(5) A Judge of the High Court may also require a service provider to keep confidential, an Order under subsection (1) and a warrant issued under subsection (1) of section 10.

(6) A service provider who without reasonable excuse fails to comply with an Order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 5,000,000,000.

Interception of content data.

15. (1) Where there are reasonable grounds to believe that the content of a specifically identified electronic communications is reasonably required for the purposes of a specific investigation in respect of a felonious offence, a Judge of the High Court may, on an application by an enforcement officer or other authorised person, order a service provider to-

(a) collect or record; or

(b) co-operate and assist a competent authority in the collection or recording of,

content data of specified communication within the jurisdiction transmitted by means of a computer system, in real time.

(2) An Order for the real-time collection or recording of content data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event not more than 30 days

(3) An application under subsection (1) shall state reasons explaining why it is believed that -

(a) the content data sought will be available with the person in control of the computer system;

(b) the type of content data suspected will be found on a computer system;

(c) an identified offence is the offence for which the warrant is sought;

(d) further disclosures are needed to achieve the purpose for which the warrant is to be issued, where authority to seek real-time collection or recording on more than one occasion is needed;

(e) measures taken shall be guided by regulations made pursuant to this Act which shall ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation;

(f) the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted;

(g) to achieve the purpose for which the warrant is being applied, real time collection or recording by a person in control of a computer system is necessary; and

(h) adequate provision is made to ensure the safe storage and protection of the content data obtained and be used solely for matters relating to investigations.

(4) A period of real-time collection or recording of content data under subsection (3) may be extended by a Judge of the High Court for a further reasonable specified period of time the same to be for an additional period not more than 30 days, on an application by an enforcement officer or other authorised person, where the extension is reasonably required for the purposes of-

(a) an investigation or prosecution;

(b) achieving the objective for which the warrant is to be issued;

(c) ensuring that the real-time collection or recording of content data is carried out whilst

maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;

(d) preventing an investigation from being frustrated or seriously prejudiced; and

(e) averting overly burdensome cost of such real-time recording and collection on the person in control of the computer system.

(5) A Judge of the High Court may also require a service provider to keep confidential, an order made under subsection (1) and a warrant issued under subsection (1) of section 10.

(6) The service provider shall have express right to challenge an order regarding the collection of real time content data where there is non-compliance with the provisions of the Act by filling an application to a Judge of the High Court.

(7) A service provider who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 5,000,000,000.

Confidentiality and Limitation of Liability.

16. (1) A service provider shall not be subject to civil or criminal liability arising in connection with its compliance with its obligation, unless it is established that the service provider-

(a) had actual notice, actual knowledge or willful and malicious intent and not merely through omission or failure to act; or

(b) had facilitated, aided or abetted the use by any person of a computer system controlled or managed by the service provider in contravention of this Act or any other law.

(2) A service provider shall not be liable under this Act or any other law for-

(a) maintaining and making his services available; or

(b) the disclosure of any data or other information to the extent required or in compliance with the exercise of powers under this Act.

Territorial jurisdiction.

17. (1) The High Court shall have jurisdiction over any violation of this Act, including any violation committed by a Sierra Leone national regardless of the place of commission.

(2) The Jurisdiction of the High Court under subsection (1), shall lie if an offence under this Act was committed -

(a) within Sierra Leone;

(b) with the use of a computer system wholly or partly situated in Sierra Leone; or

(c) when by such commission, damage is caused to a natural or juridical person who, at the time the offence was committed, was in Sierra Leone.

Prosecution of Extraditable Offences.

18. Subject to the powers of the Attorney-General and Minister of Justice, law enforcement agencies shall have power to prosecute offences under this Act. In the case of offences committed under section 24 and 26 of this Act, the approval of the Attorney-General must be obtained before prosecution.

Forfeiture to the State.

19. (1) The Court in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeits to the Republic of Sierra Leone-

(a) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence; and

(b) any computer, equipment, software, electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence;

(2) Where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Republic of Sierra Leone.

(3) The Attorney-General and Minister of Justice shall ensure that the forfeited assets or properties are effectively transferred and vested in the Republic of Sierra Leone.

(4) Any person convicted of an offence under this Act shall have his passport withheld and only returned to him after he has served the sentence or paid the fines imposed on him.

Restitution.

20. In addition to any other penalty prescribed under this Act, the Court may order a person convicted of an offence under this Act to make restitution to the victim of the false presence or fraud by directing that the person -

(a) where the property involved is money, pay to the victim an amount equivalent to the loss sustained; in any other case to-

(i) return the property to the victim or to a person designated by him; or

(ii) pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.

(b) an order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action.

PART V - INTERNATIONAL COOPERATION

Spontaneous disclosure of information.

21. (1) The Attorney-General may, subject to this Act and without prior request, forward to a foreign state, information obtained under this Act, where he considers that the disclosure of such information may-

(a) assist the foreign state in initiating or carrying out an investigation or prosecution; or

(b) lead to a request for co-operation by a foreign state.

provided that such foreign state shall have or undertake to effect mutual exchange of information with Sierra Leone in such manner as shall be agreed upon between the authorised personnel of such foreign state and the Attorney-General subject to the approval of Parliament

(2) Information provided under subsection (1), may be subject to such conditions including confidentiality, as the Attorney-General may require.

(3) Where a foreign state cannot comply with conditions required under subsection (2), it shall notify the Attorney-General, who shall determine whether the information should nevertheless be provided and where the foreign state accepts the information subject to the conditions, it shall be bound by them.

Powers of the Attorney-General.

22. (1) The Attorney-General may cooperate with any foreign state or international agency for the purpose of-

(a) investigating or prosecuting offences under this Act; or

(b) collecting electronic evidence related to an offence punishable under the laws of Sierra Leone.

(2) The Attorney-General shall communicate directly with the appropriate authority of a foreign state responsible for sending, answering, executing or transmitting requests for mutual assistance or extradition.

(3) Notwithstanding subsection (2), in case of urgency, requests may be sent directly from judicial authority to judicial authority, provided that the appropriate authority of the requested state is notified by the appropriate authority of the requesting state.

(4) For urgent request or communication, the International Police Organisation network may be used.

Authority to make and act on mutual assistance requests.

23. (1) The Attorney-General may make requests on behalf of Sierra Leone to a foreign state for mutual assistance in an investigation commenced or prosecution instituted in Sierra Leone, relating to a computer related offence or collection of electronic evidence.

(2) The Attorney-General may, in respect of a request from a foreign state for mutual assistance in an investigation commenced or prosecution instituted in that state -

(a) grant the request, in whole or in part, on such terms and conditions as may be deemed necessary;

(b) refuse the request on such conditions as he deems necessary; or

(c) postpone a request, in whole or in part, after consulting with the appropriate authority of the foreign state, on the ground that granting the request would be likely to prejudice the conduct of an investigation or prosecution in Sierra Leone.

(3) Mutual assistance requests under this section shall be effectuated-

(a) in accordance with the procedures specified by a foreign state, except where it is incompatible with the laws of Sierra Leone; or

(b) where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.

(4) The Attorney-General shall, where appropriate, before refusing or postponing assistance, after having consulted with the foreign state, consider whether the request may be granted partially or subject to such conditions, as he deems necessary.

(5) The Attorney-General shall promptly inform a foreign state of-

(a) the outcome of the execution of a request for mutual assistance;

(b) any reason that renders impossible, the execution of a request for mutual assistance or is likely to delay it significantly; or

(c) any reason for refusal or postponement of a request for mutual assistance.

(6) A foreign state may request that Sierra Leone keeps confidential the fact of any request for mutual assistance, except to the extent necessary for its execution and if Sierra Leone cannot comply with the request for confidentiality, it shall promptly inform the foreign state, which shall then determine whether the request should nevertheless be executed.

24. (1) This Act complements the Extradition Act, 1974 (Act No. 11 of 1974) which makes provision for the extradition of persons accused or convicted of an offence in another country. Extradition.

(2) Extradition shall not be requested for an offence unless it is an offence in both the foreign state and in Sierra Leone.

(3) An offence under this Act shall be extraditable if the penalty imposed is imprisonment for a term of not less than one year or a fine equivalent to the penalty of one year imprisonment.

(4) Extradition will be subject to the conditions provided for by the law of the foreign state or applicable extradition treaties, including the grounds on which the foreign state may refuse extradition.

(5) In line with the extradition or prosecution principle, where extradition is refused on the sole basis of-

(a) the nationality of the person sought to be extradited; or

(b) Sierra Leone having jurisdiction over the offence,

the investigation or prosecution shall be conducted and the matter reported to the foreign state.

Confidentiality and limitation of use.

25. Where there is no mutual assistance treaty or arrangement in force between a foreign state and Sierra Leone, Sierra Leone shall make the supply of information in response to a request on condition that it is-

(a) kept confidential; or

(b) used only for investigations or prosecutions stated in the request.

Expedited preservation of stored computer data.

26. (1) A foreign state may request or obtain the expeditious preservation of data stored by means of a computer system, located within Sierra Leone, in respect of which it intends to submit a request for mutual assistance, for the search, access, seizure, security or disclosure of the data.

(2) A request for preservation of data submitted under subsection (1) shall specify the-

(a) authority seeking the preservation of data;

(b) offence that is the subject of an investigation or prosecution, including a brief summary of the related facts;

(c) stored computer data to be preserved and its relationship to the offence;

(d) available information identifying the custodian of the stored computer data or the location of the computer system;

(e) necessity of the preservation of data; and

(f) intention to submit a request for mutual assistance for the search, access, seizure, security, or disclosure of the stored computer data.

(3) Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to expeditiously preserve the specified data in accordance with the procedures and powers under this Act.

(4) A request under subsection (1) shall be effected where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.

(5) A preservation of data effected in response to a request under subsection (1) shall be for a period not less than 90 days, in order to enable the foreign state, to submit a request for the search, access, seizure, securtiy or disclosure of the data and following the receipt of such a request, the data shall continue to be preserved until a final decision is taken on that pending request.

Expedited disclosure of preserved traffic data.

27. (1) Where during the course of executing a request under section 26, with respect to a specified communication, it is discovered that a service provider in another state was involved in the transmission of the communication, the Attorney-General shall expeditiously disclose to the foreign state, sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(2) Expedited disclosure of preserved traffic data under subsection (1) may only be withheld where the -

(a) request concerns a political offence or an offence related to a political offence; or

(b) Attorney-General considers that the execution of the request is likely to prejudice the sovereignty of Sierra Leone, security or public interest.

Mutual assistance regarding accessing of stored computer data.

28. (1) A foreign state may request the search, access, secure or disclosure of data stored by means of a computer system located within Sierra Leone, including data that has been preserved under section 26.

(2) When making a request under subsection (1), the foreign state shall provide adequate information on the following-

(a) the name of the authority conducting the investigation or prosecution to which the request relates;

(b) a description of the nature of the criminal offence and a statement setting out a summary of the relevant facts and laws;

(c) a description of the purpose of the request and of the nature of the assistance being sought;

(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in Sierra Leone, details of the offence in question, particulars of any investigation or prosecution commenced in respect of the offence, including a copy of any relevant restraining or confiscation order;

(e) details of any procedure that the foreign state wishes to be followed by Sierra Leone in giving effect to the request, particularly in the case of a request to take evidence;

(f) a statement setting out any wishes of the foreign state concerning confidentiality relating to the request and the reasons for those wishes;

(g) details of the period within which the foreign state wishes the request to be complied with;

(h) where applicable, details of the property, computer, computer system or device to be traced, restrained, seized or confiscated and of the grounds for believing that the property is believed to be in Sierra Leone;

(i) details of the stored computer data, data or program to be seized and its relationship to the offence;

(j) information identifying the custodian of the stored computer data or the location of the computer, computer system or device;

(k) an agreement on the question of the payment of the damages or costs of fulfilling the request;

(l) details to the effect that warrant in regard the matter under investigation has already been obtained to extend the investigations overseas; and

(m) any other information that may assist in giving effect to the request.

(3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute in accordance with the procedures and powers under this Act or any other law.

(4) Upon obtaining necessary authorisation under subsection (3), including a warrant to execute, the Attorney-General may seek the support and cooperation of the foreign state during such search and seizure.

(5) Upon conducting the search and seizure under subsection (4), the Attorney-General shall provide the results of such search and seizure, as well as the evidence seized, to the foreign state.

Trans-border access to stored computer data.

29. Subject to this Act, an enforcement officer or other authorized person may, without authorisation-

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

(b) access or receive through a computer system in Sierra Leone, stored computer data located in a foreign state, if such an enforcement officer or other authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.

Provided that any such access shall be without prejudice to the rights to privacy of persons and may be rescinded upon an application by a person affected to a Judge of the High Court.

Mutual assistance in real time collection of traffic data.

30. (1) A foreign state may request the Attorney-General to provide assistance in real time collection of traffic data associated with specified communications in Sierra Leone transmitted by means of a computer system.

(2) A request for assistance under subsection (1) shall specify-

(a) the authority making the request;

(b) the offence that is the subject of a criminal investigation or prosecution and a brief summary of the related facts;

(c) the name of the authority with access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose for the required traffic data;

(f) sufficient information to identify the traffic data;

(g) further details of relevant traffic data;

(h) the necessity for use of powers under this section; and

(i) the terms for the use and disclosure of the traffic data to third parties.

(3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute upon the request in accordance with the procedures and powers under this Act or any other law.

(4) Upon obtaining necessary authorisation including a warrant to execute a request under subsection (1), the Attorney-General may seek the support and cooperation of the foreign state during the search and seizure.

(5) Upon conducting the measures under this section, the Attorney-General shall provide the results of such measures as well as real-time collection of traffic data associated with specified communication to the foreign state.

Mutual assistance regarding interception of content data.

31. (1) A foreign state may, in relation to a serious offence in that state, request or provide assistance in the real time collection or recording of content data of specified communication transmitted by means of a computer system in Sierra Leone.

(2) A request for assistance under subsection (1) shall specify-

(a) the authority making the request;

(b) the offence that is the subject of a criminal investigation or prosecution and a brief summary of the facts;

(c) the name of the authority with access to the relevant communication;

(d) the location at which or nature of the communication;

(e) the intended purpose for the required communication;

(f) sufficient information to identify the communication;

(g) details of the data of the relevant interception;

(h) the recipient of the communication;

(i) the intended duration for the use of the communication;

(j) the necessity for use of powers under this section; and

(k) the terms for the use and disclosure of the communication to third parties.

(3) Upon receiving a request under subsection (1), the Attorney- General shall take appropriate action to execute the request in accordance with the procedures and powers under this Act.

(4) The Attorney-General shall, on executing the request under subsection (3), provide the results of such action as well as real time collection or recording of content data of specified communication to the foreign state.

Point of contact.

32. (1) The National Cybersecurity Coordinator or his authorized representative shall designate a point of contact available on a 24-hour, 7-days-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigation or prosecution of offences related to computer systems and data, or for the collection of evidence in electronic form.

(2) Immediate assistance to be provided under subsection (1) shall include -

(a) the provision of technical advice;

(b) the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; and

(c) the collection of evidence, the provision of legal information, and locating of suspects.

(3) A point of contact under subsection (1), shall -

(a) be resourced with and possess the requisite capacity to securely and efficiently carry out communication with other points of contact in other states, on an expedited basis;

(b) have the authority and be empowered to coordinate and enable access to international

mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.

PART VI OFFENCES

Unauthorised access.

33. (1) A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured other than to secure and protect the integrity of digital communications or for unlawful purposes, commits an offence and is liable upon conviction to fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000.

(2) For the purposes of this section, a person secures access to computer data stored in a computer system if by causing a computer system to perform a function he-

(a) alters or erases computer data; or

(b) copies, transfers or moves computer data to

(i) a computer system or computer data storage medium other than that in which it is stored; or

(ii) a different location in the same computer system or computer data storage medium in which it is stored;

(c) has the computer data output from the computer system in which it is held, whether by having it displayed or in any other manner;

(d) uses the computer data.

(3) For the purposes of this section, "unauthorised" means access of any kind, to a computer system, program or data, by a person who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than those authorised, with intent to secure access to the whole or a part of a computer system or to enable such access to be secured.

(4) The absence of authority to secure access to the whole or any part of a computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.

(5) For the purposes of this section intention or recklessness needs not relate to-

(a) a particular computer system;

(b) a particular program or data; or

(c) a program or data of any particular kind.

(6) A person shall be deemed to have contravened subsection (1)-

(a) in the absence of proof that the accused has the requisite knowledge to access the computer, program or data;

(b) notwithstanding the fact that committing the offence is impossible;

(c) in the absence of a program or data of any particular kind.

Unauthorised access to protected system.

34. (1) A person, including a corporation, partnership, or association, who intentionally or without reasonable authorisation causes a computer system to perform a function with intent to secure access to computer or program or data used directly in connection

with or necessary for a Critical National Information Infrastructure commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000.

(2) A person, including a corporation, partnership, or association, who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than that authorised, or intentionally permits tampering of such computer systems with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000.

(3) The absence of authority to secure access to the whole or any part of any computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.

Unauthorised data interception.

35. (1) A person, including a corporation, partnership, or association, who intentionally and without authorisation intercepts or causes to be intercepted non-public transmissions of data to or from a computer system whether directly or indirectly the transmission of which -

(a) results in a significant financial loss;

(b) threatens national security;

(b) causes physical injury or death to any person; or

(c) threatens public health or public safety,

commits an offence and is liable upon conviction to a fine not less than Le 100.000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

(2) Where a person, including a corporation, partnership, or association, intentionally and without authorisation, intercepts or causes to be intercepted, the transmission of data to or from a computer system over a telecommunication under subsection (1), commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

Itis immaterial whether -

(a) the unauthorised interception is not directed at-

(i) a telecommunications system;

(ii) a particular computer system;

(iii) a program or data of any kind; or

(iv) a program or data held in any particular computer system;

(b) an unauthorised interception or an intended effect of it is permanent or temporary.

Unauthorised data interference.

36. A person, including a corporation, partnership, or association, who intentionally or without authorisation does an act in relation to a computer system which-

(a) causes destruction, damage, deletion, erasure, deterioration, generation, modification or alteration of a program or data or any aspect or attribute related to the program or data;

(b) renders a program or data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the use of any program or data or any aspect or attribute related to the program or data;

(d) causes denial, prevention, suppression or hindrance of access to a program or data or any aspect or attribute related to the program or data or to any person entitled to it;

(e) causes impairment to the operation of a program;

(f) causes impairment to the reliability of any data, aspect or attribute related to a program or data;

(g) causes impairment to the security of a program or data or any aspect, attribute related to a program or data; or

(h) enables any of the acts mentioned in paragraphs (a) to (g) to be done,

commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of

imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

Unauthorised system interference.

37. A person, including a corporation, partnership, or association, who intentionally or without authorisation does an unauthorised act in relation to a computer system which -

(a) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the functioning of a computer system;

(b) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the communication between or with a computer system;

(c) interferes with or hinders access to acomputer system;

(d) impairs the operation of a computer system;

(e) impairs the reliability of a computer system;

(f) impairs the security of a computer system; or

(g) enables any of the acts mentioned in paragraphs (a) to (f) to be done,

commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

Provided that it shall not be an offence if interference with a computer system is undertaken in compliance and in accordance with the terms of a warrant issued under this Act or any law.

Misuse of device.

38. (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation manufactures, adapts, sells, procures for use, receives, possesses, imports, offers to supply, distributes or otherwise makes available-

(a) a device designed or adapted primarily for the purpose of committing an offence under this Act; or

(b) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, designed or adapted primarily for the purposes of a computer system.

(c) uses electronic communication equipment to bypass standard inter-connection path by illegal redirection of traffic.

commits an offence and is liable upon conviction to a fine not less than Le 500.000,000 and not more than Le 1,500,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 3,000,000,000 and not exceeding Le 6,000,000,000.

(2) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act under subsection (1),-

(a) for the purpose of training, testing or protection of a computer system; or

(b) in compliance of and in accordance with the terms of a judicial order issued or in exercise of a power under this Act or any law.

(3) For the purpose of subsection (1), possession of a program or a computer password, access code, or similar data includes having-

(a) possession of a computer system which contains the program or a computer password, access code, or similar data;

(b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or

(c) control of a program or a computer password, access code, or similar data that is in the possession of another person.

Unauthorised disclosure of password.

39. A person, including a corporation, partnership, or association, who intentionally or without authorisation discloses to another person a password, access code or other means of gaining access to any program or data held in a computer system-

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) to occasion any loss,

commits an offence and is liable upon conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 50,000,000 and not exceeding Le 100,000,000.

Computer related forgery.

40. (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly

readable or intelligible, commits an offence and is liable upon conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 50,000,000 and not exceeding Le 100,000,000

(2) A person, including a corporation, partnership, or association, who dishonestly or with similar intent -

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any economic benefit for oneself or for another person,

intentionally or without authorisation inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable or intelligible commits an offence and is liable on conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 year and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000

Computer fraud.

41. A person, including a corporation, partnership, or association, who intentionally causes loss of property, valuable security or consideration to another person by -

(a) inputting, alteration, modification, deletion, suppression or generation of a program or data;

(b) interference, hindrance, impairment or obstruction with the functioning of that computer system; or

(c) copying, transferring or moving data or program to another computer system, device or storage medium other than that in which it is held or to a different location in any other computer system, device or storage medium in which it is held;

(d) using any data or program; or

(e) having any data or program output from thecomputer system in which it is held, whetherby having it displayed or in any other manner,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for himself or for another person commits an offence and is liable upon conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100, 000,000 and not exceeding Le250,000,000"

Identity theft and impersonation.

42. (1) A person, including a corporation, partnership, or association, who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft, phishing of its employer, staff, service providers and consultants with the intent to defraud commits an offence and is liable upon conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 3 years and not exceeding 7 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000.

(2) A person, including a corporation, partnership, or association, who fraudulently-

(a) or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person; or

(b) impersonates another entity or person, living or dead, with intent to-

(i) gain advantage for himself or another person;

(ii) obtain any property or an interest in any property;

(iii) cause disadvantage to the person or entity being impersonated or another person; or

(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and is liable upon conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 3 years and not exceeding 7 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000.

(3) A person, including a corporation, partnership, or association, who makes or causes to be made, either directly or indirectly, any false news as a material fact in writing, knowing it to be false and with the intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person commits an

offence and shall be liable on conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 3 years and not exceeding 7 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000

Electronic signature.

43. A person, including a corporation, partnership, or association, who with the intent to defraud and or misrepresent, forges through electronic devices another person's signature or company mandate commits an offence and shall be liable on conviction to a fine not less than Le 50,000,000 and not more than Le 1,000,000,000 or to a term of imprisonment not less than 3 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 5,000,000,000.

Cyber stalking and cyber bullying.

44. (1) A person, including a corporation, partnership, or association, who individually or with another person, willfully and repeatedly communicates, either directly or indirectly, with another person, if he knows or ought to have known that his conduct -

(a) is likely to cause that person apprehension or fear of violence to him or damage or loss on his property; or

(b) detrimentally affects that person;

commits an offence and shall be liable on conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000

(2) A person, including a corporation, partnership, or association, who recklessly or intentionally sends a message or other matter by means of a computer system or network that-

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so disseminated without consent; or

(b) he knows to be false, for the purpose of causing danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent,

commits an offence and shall be liable on conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000.

(3) Notwithstanding subsection (1) a person shall not be deemed to have acted in contravention of this Act if he does an act -

(a) for the purpose of preventing or detecting crime;

(b) in compliance of and in accordance with the terms of a judicial order issued or in exercise of any power under this Act or any law; or

(c) which is in the interest of the public.

Cyber Squatting.

45. (1) A person, including a corporation, partnership, or association, who intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by an individual, body corporate or belonging to a government institution in Sierra Leone, on the internet or any other computer network, without authority, right or reasonable excuse and for the purpose of interfering with the use by the owner, registrant or legitimate prior user, shall be liable to damages in a civil action as determined by a Judge of the High Court.

(2) In awarding penalty against an offender under this section, a court shall have regard to the following-

(a) refusal by the person to relinquish, upon formal request by the rightful owner without reasonable excuse of a name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to the Government of Sierra Leone; or

(b) any attempt by the offender to obtain compensation in any form for the release to the rightful owner for use of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by the individual, body corporate or belonging to the Government of Sierra Leone.

(3) In addition to the penalty specified in this section, the court may make an order directing an offender to relinquish such registered name, mark, trademark, domain name or other word or phrase to the rightful owner.

Infringement of copyright and related rights.

46. A person, including a corporation, partnership, or association, who, through input, alteration, modification, deletion, suppression or generation of a program or data or through use of a computer, computer system or electronic device willfully infringes any right protected under the Copyright Act, 2011(Act No. 8 of 2011) or any law in force for protection of copyrights and related rights, commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000 without prejudice to civil remedies that may be available.

Online child sexual abuse.

47. (1) A person, including a corporation, partnership, or association, who, intentionally-

(a) distributes, produces, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, prints, photographs, copies, provides location, requests for, offers in any other way, or makes available in any way child pornography through a computer system or storage data medium; or

(b) acquiesces a child's participation in pornography,

commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

(2) A person, including a corporation, partnership, or association, who intentionally poses, grooms or solicits, through any computer system or network, to meet a child for the purpose of -

(a) engaging in sexual activity with the child;

(b) engaging in sexual activity with the child where-

(i) coercion, inducement, force or threat is used;

(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or

(iii) a child's mental or physical disability or situation of dependence is a b u s e d;

commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement.

(4) For purposes of this section-

"child" means a person under the age of 18 years;

"child pornography" includes data which, whether visual or audio, depicts-

(a) a child engaged in sexually explicit conduct;

(b) a person who appears to be a child engaged in sexually explicit conduct; or

(c) realistic images representing a child engaged in sexually explicit conduct.

48. (1) A person, including a corporation, partnership, or association who: Online adult sexual abuse.

(a) take or share an intimate image or voice material of a depicted person without his/her consent;

(b) take or share an intimate image or voice material of a depicted person without his/her consent, with the intention to humiliate, alarm or distress the victim;

(c) take or share an intimate image or voice material of a depicted person without his/her consent, for the purpose of either sexual gratification by the perpetrator or that of another;

(d) threaten to share any intimate image or voice material of a depicted person with intent to cause the depicted person to fear that the image or audio material will be shared, or being reckless as to whether the depicted person will have such fear that the threat will be executed;

(e) disseminate or post sexually explicit image, media or voice material without the consent of the depicted person, whether or not the intent is to shame, humiliate, frighten or cause the depicted person harm.

commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation,

partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

(2) In this section, the expressions "intimate image or voice material" shall include video, images or voice media created by the depicted person which he/she has not willingly put into the public domain; video, images or voice media taken by another; video, images or voice media in the possession of the perpetrator by any means whatsoever including been stolen from a hacked computer or other digital device of the depicted person; video, image or voice material that may have been doctored by superimposing the face or voice of a depicted person unto an existing intimate or sexually explicit image or some other voice media.

Attempting and Aiding or Abetting.

49. (1) A person, including a corporation, partnership, or association, who intentionally abets the commission of, aids to commit, attempts to commit or does any act preparatory to or in furtherance of the commission of an offence under this Act commits an offence and is liable upon conviction to the same penalty as that prescribed in respect of the substantive offence under this Act.

(2) An offence may be deemed to have been committed under subsection (1), notwithstanding where the act in question took place.

Registration of cyber cafes.

50. (1) No person shall engage in the operation of a business of providing computers for accessing the internet, playing games, chatting or doing other computer-related tasks unless the business.

(a) has a registered business name with the Corporate Affairs Commission established under the Companies Act, 2009 (Act No. 5 of 2009); or

(b) is registered with a local council; or

(c) is registered with the office of the Administrator and Registrar General; and

(d) registered with National Telecommunications Commission established under the Telecommunications Act, 2006 (Act No. 9 of 2006) as a business concerned with providing computer access to the internet.

(2) A person, including a corporation, partnership, or association, who perpetrates electronic fraud or online fraud under this Act using a cybercafé, commits an offence and is liable on conviction to a fine not less than Le 50,000,000 and not more than Le 500,000,000 or to a term of imprisonment not less than 3 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 5,000,000,000.

provided that the cybercafé owner or manager shall not be liable for such an offence unless there is evidence to the effect that he or she or it were complicit in the commission of the offence.

Cyber Terrorism.

51. (1) A person who accesses or cause to be accessed a computer or computer system or network for purposes of a terrorist act, commits an offence and is liable on conviction to a term of imprisonment not less than 10 years and not exceeding 20 years.

(2) For purposes of this section, "terrorist act" shall have the same meaning as provided under the Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012 (Act No. 2 of 2012).

Racist Xenophobic Offences.

52. (1) A person, including a corporation, partnership, or association, who with intent-

(a) distributes or otherwise makes available, racist or xenophobic material to the public through a computer system or network;

(b) threatens through a computer system or network any other person or group of persons for the reason of belonging to a group distinguished by race, colour, descent, national or ethnic origin, gender religion, as well as disability

(c) insults publicly through a computer system or network any other person or group of persons distinguished by race, colour, descent or national or ethnic origin, as well as religion; or

(d) distributes or otherwise makes available, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity,

commits an offence and is liable upon conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le250, 000,000 and not exceeding Le 500,000,000

Reporting cyber threats.

53. (1) A person or institution that operates a computer system or network, whether public or private, shall immediately inform the National Computer Security Incidence Response Team of an attack, intrusion and other disruption liable to hinder the functioning of another computer system or network, and the National Computer Security Incidence Response Team shall take necessary and appropriate measures to protect computer systems and networks.

(2) In order to protect a computer system or network under subsection (1), the National Computer Security Incidence Response Team may propose the isolation of an affected computer system or network pending the resolution of the issues.

(3) A person or institution who intentionally or without reasonable excuse fails to report an incident of an attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network to the National Computer Security Incidence Response Team within 7 days of its occurrence, commits an offence and is liable on conviction to a fine not less than Le

10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le50,000,000 and not exceeding Le 100,000,000.

Breach of confidence by service providers.

54. (1) A person or institution which, being a computer based service provider and or vendor does an act with intent to defraud and by virtue of his position as a service provider, forges, illegally uses security codes of the consumer with the intent to gain a financial and or material advantage or with intent to provide less value for money in his or its services to a consumer commits an offence and upon conviction is liable to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000.

(2) Where an offence under this Act committed by a body corporate is proved to have been committed on the instigation or with the connivance of or attributable to willful neglect on the part of a director, manager, secretary or other like officer of the body corporate or any officer purporting to act in any such capacity, he, as well as the body corporate, where practicable, shall be deemed to have committed the offence.

(3) Notwithstanding subsection (1), where a body corporate is convicted of an offence under this Act, which threatens national security the Court may in the case of multiple or repeated

offenders, order that the body corporate shall be wound up and all its assets and properties forfeited to the state, without prejudice to any liability owing from the said body corporate being first satisfied.

(4) Nothing contained in this section shall render a person liable to punishment, where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.

Employees responsibility.

55. (1) Without prejudice to any contractual agreement between an employer and employee, an employee shall relinquish or surrender all codes and access rights to his employer within a reasonable time in his possession, power or control upon disengagement from employment.

(2) An employee who, without any lawful reason, continues to hold unto the code or access right of his employer after disengagement without any lawful reason commits an offence and shall be liable on conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le50,000,000 and not exceeding Le 100,000,000

Corporate liability.

56. (1) A natural person, who exercises management or supervisory authority, based on-

(a) power of representation of a legal person;

(b) authority to take decisions on behalf of a legal person;

(c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person,

and fails to exercise reasonable and proper control over such legal person commits an offence under this Act, and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000.

(2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act.

Acts by children.

57. Without prejudice to the offences prescribed under this Act and subject to the provisions of the Children and Young Persons Act Cap.44 and the Child Rights Act 2007, where an act done by a child would be deemed to be an offence under this Act such child shall be treated as a juvenile and dealt with accordingly

PART VII -MISCELLANEOUS PROVISIONS

Regulations.

58. The Minister may by Statutory Instrument make Regulations as it considers necessary or expedient for giving effects to any of the provisions of this Act.

Passed in Parliament this *th day of July,* in the year of our Lord two thousand and twenty one.

PARAN UMAR TARAWALLY,
Clerk of Parliament.

THIS PRINTED IMPRESSION has been carefully compared by me with the Bill which has passed Parliament and found by me to be a true and correct printed copy of the said Bill.

PARAN UMAR TARAWALLY,
Clerk of Parliament.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTING DEPARTMENT, SIERRA LEONE.