GUIDELINE FOR A MODEL CYBERSECURITY LAW

A Guideline for a model law on computer enabled and computer related crimes in the African Union Member States.

PART I- INTRODUCTION

This Guideline provides guidance to African Member States for designing cybersecurity legislation and explains the key features and benefits of a standard cybersecurity law.

1. The Guideline

The implementation of cybersecurity is an essential component of regional response to ensuring cybersecurity in Africa. The seventh key action in the United Nations Road Map for Digital Cooperation is 'promoting trust and security in the digital environment'.[1] Following endorsement by the 2019 Sharm El Sheikh Declaration,[2] in February 2020, the African Union Commission (AUC) adopted the Digital Transformation Strategy for Africa.[3] The African Digital Transformation Strategy[4] has highlighted the need for a greater capacity to detect and mitigate cyber-attacks. Following the strategy, the responsibility of African governments to create an enabling environment with policies and regulations that promote digital transformation across foundational pillars - which includes cyber security - is fundamental.[5] The Strategy also states unequivocally, that "collaborative ICT regulatory

[1] United Nations General Assembly. Report of the Secretary-General Roadmap for Digital Cooperation A/74/81 June 2020. Roadmap_for_Digital_Cooperation_EN.pdf (un.org).
[2] African Union Specialized Technical Committee on Communication and Information Technologies (STC-CICT) Third Ordinary Session, 22 - 26 October 2019, Sharm El Sheikh, Egypt 37590-2019_sharm_el_sheikh_declaration_-_stc-cict-3_oct_2019_ver2410-10pm-1rev-2.pdf (au.int)
[3] The African Union Digital Transformation Strategy for Africa (2020-2030).
[4] The African Union Digital Transformation Strategy for Africa (2020-2030).
[5] The African Union Digital Transformation Strategy for Africa (2020-2030). Pg. 7

measures and tools are the new frontier for regulators and policy makers as they work towards maximizing the opportunities afforded by digital transformation across industries".[6] Digital transformation offers Africa tremendous opportunities, however, effective, and efficient digital transformation in Africa can only be achieved with cybersecurity.

It is necessary to develop guidelines for a model law that can provide assistance to African Member States in the drafting of cybersecurity legislation which are compatible with best practices. In order to ensure a minimum set of baseline standards by which African governments can address cybersecurity, this guideline has undertaken an assessment of legislation and treaties on cybersecurity. This guideline has been produced with adequate consideration of existing national cybersecurity legislation in Africa, the African Union Convention for Cybersecurity and Personal Data Protection (Malabo Convention) 2014; the Convention on Cybercrime (Budapest Convention) 2001; and the United Nations Norms of Responsible State Behaviour in Cyberspace and also draws on other existing and proposed regional and international efforts on cybersecurity, including the proposed and ongoing efforts to elaborate a United Nations Global Convention on Countering the Use of ICTs for Criminal Purposes.

2. **Object of the Guideline**

This guideline is not a binding law or legislation, but rather a set of guiding principles which African Member States may follow as they set out to establish standards for ensuring cybersecurity or cybercrime laws. This guideline does not limit the operation of any national or regional law, which is already in existence, or may come into existence in future, that expressly or impliedly regulates

[6]The African Union Digital Transformation Strategy for Africa (2020-2030). pg. 7. Italics mine for emphasis.

cybersecurity and prohibits any activity regarded as cybercriminal offences in any jurisdiction. The guideline does not attempt to provide specific legislative language for stipulating the provisions of cybersecurity or cybercrime laws, or the implementation of such laws, and leaves the precise language to the discretion of African States in respect of the sovereignty of states, and recognising that African states may vary in terms of legal systems.

3. **Purpose of the Guideline**

Cybersecurity legislation covers the regulation, maintenance and promotion of cybersecurity activities, critical national infrastructure and computer-related services. The guideline is designed to assist African Member States in drafting, reforming and modernizing their cybersecurity laws so as to take into account the particular features and needs of promoting cybersecurity in the region. This guideline is for African States, African policymakers and legislators who wish to understand the valuable components of a model cybersecurity law.

This guideline attempts to bridge the best practice principles of substantive offences, powers, and mutual legal assistance, such as those enunciated in regional and international cybersecurity treaties, with specific examples of standards, principles and measures that elaborate the various elements that need to be included in a cybersecurity legislation. It also provides guidelines for provisions in relation to principles such as the respect for human rights, law enforcement standards and judicial or other oversight. Poorly drafted cybersecurity laws that diverge from international best practice can have a negative effect on efforts to address cybersecurity, and regional and international cooperation. Ineffectively drafted model laws can also cause countries to enact inadequate cybercrime legislation, whilst at the same time, criminalizing and labelling conduct as cybercrime which other countries may not view as

cybercrime, hence, the importance of following an appropriate model for developing cybersecurity legislation.

This guideline addresses standard cybersecurity measures including recognising offences and illustrates the types of acts than can be criminalised under a model cybersecurity law. The guideline calls on States, lawmakers and regulators to provide guidance for creating cybersecurity programs that are flexible, scalable, practical, and consistent with global best practices. Ultimately, this guideline identifies recommendations on standards for cybersecurity laws and regulation in respective African jurisdictions. It also provides guidance on law enforcement activities for ensuring cybersecurity which underscore the respect for human rights in accordance with international and regional human rights standards.

4. **Definition of Terms**

(1) "Competent authority" shall mean a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under the national cybersecurity legislation with respect to specific criminal investigations or proceedings.

(2) "Computer data" shall mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function.

(3) "Computer extortion" shall mean an attack or a threatened attack accompanied with a demand for money or some other response in return for remediating or stopping the attack.

(4)“Computer system” shall mean any device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data.

(5)“Corporation” shall mean a limited liability undertaking within the meaning of the applicable national legislation of a Member State.

(6)“Critical infrastructure” shall mean and include all of the assets, systems and networks – physical and virtual – that are essential to the proper functioning of a nation’s economy, national public health or safety, security, or any combination of the above.

(7)“Cybercrime” shall mean, for the purpose of this Guideline, the conduct as defined in Part II-General Offences.

(8)“Cybersecurity” shall mean state of protection against the criminal or unauthorized uses of computer systems and data, the measures taken to achieve this and the activities necessary to protect network and information systems and the users of such systems, and other persons affected by cyber threats.

(9)“Cybersquatting” shall mean registering, selling or using a domain name with the intent of profiting from the goodwill of another person’s trademark or business reputation.

(10) “cyber threat” shall mean any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

(11) "Data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the

purpose and means of processing of personal data.

(12) "Denial of Service Attacks" shall mean activities that prevents a rightful user from accessing a computer system, or rapid and continuous online requests which are sent to a target server in order to overload the computer servers.

(13) "Fraudulent inducement" shall mean deceitful practices in order to persuade another party to act against their best interest in a manner that causes the other party to act to the advantage of the party engaging in the deceitful practice.

(14) "Guideline" shall mean suggested cybersecurity legislative content for African Member States, designed by UNECA that is not part of a nation's legislative body and aimed at supporting the introduction of new legislation or reforming existing law.

(15) "Interception" shall mean monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system over a telecommunications system, and includes, in relation to a function of a computer system, listening to or recording a function of a computer system or acquiring the substance, its meaning or purport of such function.

(16) "Malware and viruses" shall mean a set of computer instructions that are designed to infect computer programs or computer data, modify, destroy, record, or transmit data, and disrupt normal operation of a computer system.

(17) "Officer", in relation to a corporation, shall mean any director, partner, chief executive, manager, secretary or other similar officer of the corporation, and includes any person purporting to act in any such capacity;

and for a corporation whose affairs are managed by its members, any of those members as if the member were a director of the corporation.

(18) “Personal data” shall mean information relating to an identified or identifiable natural person.

(19) “personal or human identifier” shall mean a subset of personally identifiable information and data elements, which identify an individual and can permit another person to assume that individual's identity without their knowledge or consent.

(20) “Ransomware” shall mean computer malware that is installed covertly on a computer system, computer programme or computer data to prevent access to it.

(21) "Requested State" shall mean State being requested to provide legal assistance.

(22) "Requesting State" shall mean a Member State requesting for legal assistance and may include an international entity to which a Member State is obligated.

(23) “Safe-Habour” shall mean a national legal provision that will shield an individual or entity in certain circumstances from being held liable for activities.

(24) "Service provider" shall mean a public or private entity that provides to users of its services the means to communicate by use of a computer system; and any other entity that processes or stores computer data on behalf of that entity or its users.

(25) “State of mind” of a person shall mean the knowledge, intention, opinion, belief or purpose of the person; and the person’s reasons for the intention, opinion, belief or purpose.

(26) "Unauthorized access" shall mean trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without lawful consent.

(27) “Vulnerable Person” shall mean a natural person who due to particular characteristics is susceptible to being disadvantaged including due to age, disability, gender or location.

5. **Key Provisions**

Part I

Introduction

1. The Guideline
2. Object of the Guideline
3. Purpose of the Guideline
4. Definition of Terms
5. Key Provisions

Part II

6. General Scope

Part III

General offences

7. Illegal and Unauthorized Access
8. Illegal Interception
9. Misuse of Computer Devices and Access Codes
10. Unauthorized Modification of Computer Programme or Data
11. Unauthorized Interference with Computer Systems
12. Child Pornography
13. Misleading Content Targeted at Children
14. Offences in Relation to Identity
15. Denial of Service Attacks
16. Ransomware and Computer Extortion
17. Fraudulent Inducement
18. Online Infringements of Copyright and Related Rights
19. Cybersquatting
20. Unlawful Obtaining of Personal Data

Part IV

Criminal Procedure and Determination of Liability

21. Criminal Intent
22. Criminal Negligence
23. Attempt, Aiding and Abetting and Conspiracy
24. Liability of Persons
25. Offences by Corporations

Part V

Criminal Procedure and Law Enforcement

26. Procedural and Substantive Powers
27. Scope of procedural Measures
28. Conditions and Safeguards
29. Preservation and Disclosure of Computer Data
30. Production and Obtaining of Computer Data
31. Search and Seizure of Stored Computer Data
32. Authorised Warrants
33. Blocking Filtering and Removal of Illegal Content
34. Jurisdictional Scope

Part VI

Cybersecurity Cooperation

35. Cooperation and Mutual Legal Assistance
36. Measures to Enhance Law Enforcement Cooperation
37. International Cooperation
38. Public Private Partnership

Part VII

Cybersecurity Management

39. Critical Infrastructure
40. Computer Emergency Response
41. Cybersecurity Points of Contact
42. Cybersecurity Strategies and Framework
43. Establishment of a Central Authority for Cybersecurity Regulation

PART II – GENERAL SCOPE

6. (1) The scope of cybersecurity legislation of Member States must focus on the prevention, investigation and prosecution of cyber dependent and cyber enabled offences which are criminalised within statute established in accordance with the national legislation of Member States.

(2) Member States cybersecurity legislation must respond to, manage, and prevent cybersecurity threats or incidents that occur within and outside the country that may threaten the safety of life and property of citizens and residents and the national security and defence of the state.

(3) Generally, cybersecurity law covers cyber services essential for the functioning of society, state, local authorities, network and information systems and critical infrastructure, and should adequately impose compulsory organizational, physical and information security measures Member States must take for preventing, mitigating and resolving cyber threats and incidents.

(4) Member States must ensure that national cybersecurity legislation prioritise the protection of human rights and fundamental freedoms whilst employing measures to prevent and combat cybercrime, ensure public-private partnership, and encourage states to engage in public education, research, and training to enhance the knowledge and skills pertaining to cybersecurity.

PART III- GENERAL OFFENCES

Illegal and Unauthorised Access

7. (1) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without authorisation or exceeding authorisation, access to the whole or any part of a computer system or in relation to a computer system that is connected to another computer system, or obtains, alters, or prevents authorised access.
(2) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without authorisation or exceeding authority, causing a computer to perform any function to obtain, secure or prevent access to a computer programme, system or data held in that computer.

Illegal Interception

8. Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, without authorisation and without lawful excuse or justification, the interception of computer data by technical means to, from or within a computer system, including in relation to a computer system that is connected to another computer system.

Misuse of Computer Devices and Access Codes

9. Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and

without justification the production, sale, procurement for use, possession, importation, distribution of the following:

a) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in the national legislation as a cyber-criminal offence
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, with intent that it be used for the purpose of committing any of the offences established in the national legislation as a cyber-criminal offence.

Unauthorised Modification of Computer Programme or Data

10.(1) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the intentional, and direct or indirect unauthorised modification of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

(2) A modification of a computer programme or data will suffice if:

(a) a programme or data held in the computer is damaged, altered, erased without authorisation or,

(b) a programme or data is added to or removed from a programme or electronic record held in the computer system or,

(c) an act occurs which impairs or deteriorates the normal operation of any computer or programme therein.

(3) It shall be immaterial that the unauthorised modification or interference is, or is intended to be, permanent or merely temporary.

Unauthorised Interference with Computer Systems

11.(1) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, without authorisation and without lawful excuse or justification the interference with the functioning of a computer system or hindering a person who is lawfully using or operating a computer.

(2) Interference or hinderance includes but is not limited to:

(a) preventing the functioning of the computer system by any means,

(b) causing electrical, electronic and electromagnetic interference to a computer system,

(c) causing denial of service attacks,

(d) defacing computer systems,

(e) corrupting a computer system by any means including through the use of malware and viruses.

(3) It shall be immaterial that the unauthorised interference is, or is intended to be, permanent or merely temporary.

Child Pornography

12.(1) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally or negligently in relation to the protection of children the following acts:

(a) publishing child pornography through a computer system;

(b) distributing child pornography through a computer system

(c) production of child pornography for the purpose of its publication through a computer system or,

(d) possession of child pornography in a computer system or on a computer data storage medium

(2) "child pornography" includes material that visually depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; (c) images representing a child engaged in sexually explicit conduct; and (d) unauthorised images of nude children;

(3) "child" shall mean a person below eighteen years or as otherwise defined in national legislation;

(4) "publish" means (a) transmit, disseminate, circulate, deliver, exhibit;

(5) “distribute” means exchange, barter, lend, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(6) “possession” means have in possession or custody, or under control; and,

(7) “produce” means print, photograph, copy or make in any other manner whether of the same or of a different kind or nature.

Misleading Content Targeted at Children

13. Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences the use of misleading words or digital images on the internet targeted at children and aimed at grooming children to enable the commission of criminal acts including the creation of domain names on the internet to deceive minors to enable to commission of acts which national legislations may consider as criminal acts.

Offences in Relation to Identity

14. (1) Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences when committed intentionally the following acts:

(a) Assuming the identity of another person (whether living, deceased, natural or corporate) with or through a computer system or in relation to other standards stipulated in the national laws.

(b) The obtaining, disclosing or procuring of the 'personal data' or 'personal or human identifier' of a living or deceased person in order to assume the identity of such person with the intent to commit, or facilitate the commission of a criminal offence with or through access to a computer system.

Denial of Service Attacks

15.(1) Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences when committed intentionally the following acts:

(a) flooding the bandwidth or resources of a targeted computer system or servers with traffic, thereby preventing the legitimate users from accessing information or services.

(b) compromising and taking control of multiple computers with security flaws in order to use them to commit the act in paragraph 1.

Ransomware and Computer Extortion

16.Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional installing of malware and viruses covertly on a computer system thereby preventing access to it, followed by demands for a ransom payment in exchange for returning access or not publishing or exposing data held on the computer system.

Fraudulent Inducement

17. Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional and fraudulent sending of unrequested or unsolicited messages by electronic means, or the creation of deceptive websites or internet hyperlinks to lure personal or financial information from unsuspecting victims with the intent to use such information for fraudulent purposes or other purposes of beneficial interests .

Online Infringement of Copyright and Related Rights

18. Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law the online infringement of copyright, including the liability of intermediaries where they act outside the safe-harbour domain.

Cybersquatting

19. Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law the intentional taking or making use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right and with the intent for beneficial interests.

Unlawful Obtaining of Personal Data

20. Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law for;

(1) A person knowingly or recklessly to-

(a)obtain or disclose personal data without the consent of a data controller;

(b)procure the disclosure of personal data to another person without the consent of the data controller; or

(c)after obtaining personal data, retains it without the consent of the person who was the data controller in relation to the personal data when it was obtained.

(2) sell or offer for sell personal data if the person obtained the data in circumstances stated in paragraph (1).

(3) Paragraph (1) may not apply if the obtaining, disclosing, procuring or retaining-

(a)was necessary for the purposes of preventing or detecting crime;

(b)was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or

(c)in the particular circumstances, was justified as being in the public interest.

PART IV: CRIMINAL PROCEDURE AND DETERMINATION OF LIABILITY

Criminal Intent

21. Member States shall adopt such legislative and other measures as may be necessary to establish intent where a person through computer enablement whether in part or in whole is deemed to intend to cause or contributes to causing an offence established in the national legislation as an offence which results from the use or intervention of the computer system.

Criminal Negligence

22. Member States shall adopt such legislative and other measures as may be necessary to establish criminal negligence where a person through computer enablement whether in part or in whole is deemed to have caused an event negligently, if without intending to cause the event, the person causes it by voluntary action from the use or intervention of computer system without due care as would reasonably be necessary under such circumstances.

Attempt, Aiding and Abetting and Conspiracy

23. (1) Member States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, and attempt to commit of any of the cyber offences established in the national legislation.

(2) Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with national law as cyber offences.

(3) Member States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, conspiracy to commit an offence established in accordance with national law as cyber offences, whether the medium used in whole or in part was cyber enabled.

Liability of Persons

24. (1) Member States shall ensure compliance and effective enforcement of cybersecurity legislation by imposing convictions, sentencing and punitive measures for commission of offences outlined within the legislation.

(2) Member States shall adopt such legislative and other measures as may be necessary, consistent with and subject to its domestic laws, to ensure that

legal persons other than the State and public institutions can be held liable for offences established in national cyber security legislations which are committed on their behalf by their organs or representatives.

(3) Such liability may be criminal, civil or administrative and shall not exclude or be without prejudice to the criminal liability of the natural persons who have committed such offences.

(4) Member States shall make the commission of an offence established in accordance with their national cybersecurity laws liable to effective, necessary and proportionate sanctions for both natural and legal persons.

Offences by Corporations

25. (1) Member States may ensure that in a proceeding for an offence under the national cybersecurity legislation, it shall be evidence that the corporation had that state of mind in relation to a particular conduct with evidence that-

(a) an officer, employee or agent of the corporation engaged in that conduct within the scope of his or her actual or apparent authority; and

(b) the officer, employee or agent had that state of mind.

(2) Where a corporation commits an offence stipulated as a cyber-criminal offence under the national legislation,

(a) a person who is-

i. an officer of the corporation, or a member of the corporation (in the case where the affairs of the corporation are managed by its members); or

ii. an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence; and

(b) a person who-

i. consented, connived or conspired with others, to effect the commission of the offence;

ii. is in any other way, whether by act or omission, intentionally party to, the commission of the offence by the corporation; or

iii. knew or ought reasonably to have known that the offence by the corporation would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence;

shall be liable of that same offence as is the corporation.

PART V - CRIMINAL PROCEDURE AND LAW ENFORCEMENT

Procedural and Substantive Powers

26. Member States shall develop and maintain an effective and rule of law-based national criminal justice system that can ensure that any person prosecuted for offences covered in the national cybersecurity legislation is brought to justice whilst ensuring full protection of human rights and fundamental freedoms in accordance with the African Charter on Human and Peoples' Rights and other international human rights instruments.

Scope of Procedural Measures

27. (1) Member States shall adopt such legislative and other measures as may be necessary to establish the powers and procedures necessary for the purpose of specific criminal investigations or proceedings.

(2) Member States shall apply such powers and procedures to:

(a) the offences established in their national legislation as cyber-criminal offences;

(b) the collection of evidence in electronic or digital form of a criminal offence established in their national legislation as cyber-criminal offences.

Conditions and Safeguards

28. Member States shall ensure that the establishment, implementation and application of powers and procedures are subject to conditions and safeguards provided for under its domestic law, which shall provide for the total protection of human rights and fundamental freedoms, in line with international and regional human rights standards including rights arising pursuant to obligations Member States may have ratified under the African Charter on Human and Peoples' Rights.

Preservation and Disclosure of Computer Data

29. Subject to appropriate standards and legal domestic considerations, Member States may adopt measures as may be necessary to enable its competent authorities to order the preservation and disclosure of data, that have been stored by means of a computer programme or system, in particular where such data is relevant for investigation purposes, law enforcement of judicial processes.

Production and Obtaining of Computer Data

30. Member States shall adopt measures as may be necessary to empower its competent authorities to order: a) persons in its territory to submit specified computer data in that person's possession or control and b) a service provider offering its services in the territory to submit data or information relating to such services or service users in their possession or control.

Search and Seizure of Stored Computer Data

31. (1) Member States shall adopt measures as may be necessary to empower its competent authorities to search or access: a) a computer system or part of it and computer data stored therein; and b) a computer-data storage medium in which computer data may be stored in its territory

(2) Member States shall adopt measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, and have grounds to believe that the data sought is located or stored in another computer system, or is connected to or forms part of another computer system in its territory, and such data is lawfully accessible from, or available to the initial system, the authorities shall be granted powers within lawful standards to extend the search or accessing to the other computer system.

(3) Member States shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or take in their possession where necessary such computer data accessed. These measures shall include the power to: a) a seize or similarly secure a computer system or part of it or a computer-data storage medium; b) make and retain a copy of those computer data; c) facilitate the integrity of the relevant stored

computer data; d) render inaccessible or remove those computer data in the accessed computer system.

Authorised Warrants

32.(1) Member States shall authorize competent authorities upon application to a competent court of appropriate jurisdiction to issue an interception warrant to facilitate the demand for, collection and/ or recording of computer data where such specified data is necessary for law enforcement, criminal investigation or criminal proceedings.

(2)Member States shall provide that upon satisfaction on the basis of an application to a court of competent jurisdiction by a law enforcement officer, that a specified computer data is reasonably required for the purpose of a criminal investigation or criminal proceedings, the court may order that: (a) a person in control of a computer system produce the specified computer data; and (b) an internet service provider produce specified computer data or produce information about persons who subscribe to or otherwise use the service.

Blocking Filtering and Removal of Illegal Content

33.Taking into account the principles of legitimacy, necessity and proportionality, Member States may adopt such legislative and other measures as may be necessary to provide powers to competent authorities for the blocking, filtering, and taking down of illegal content on the order of a court on certain specified legal grounds for the purpose of ensuring cybersecurity or for the purposes of ensuring the respect of the rights of citizens in relation to cyber enabled criminal activities.

Jurisdictional Scope

34.(1) Member States shall adopt such measures as may be necessary to exercise criminal jurisdiction over the cyber enabled offences established in accordance with their national laws if:

a) The offence is committed in the territory of that Member State,

b) The offence is committed on board a vessel that is flying the flag of that Member State or an aircraft registered under the laws of that Member State at the time to offence is committed, or

c) The offence is committed by one of its nationals, if the offence is punishable under the national cybercrime law where it was committed or if the offence is committed outside the territorial jurisdiction of any Member State.

(2) Member States may also establish its jurisdiction over any such offence when:

a) The offence is committed against a national of that Member State;

b) The offence is committed by a national of that Member State or a stateless person who has his or her habitual residence in its territory.

(3) Member States may also adopt such measures as may be necessary to establish jurisdiction over the offences covered by their national cybersecurity legislation when the alleged offender is present in its territory and the state does not extradite the offender on the grounds of nationality after a request for extradition.

(4) Having regard to the principle of double criminality, Member States intending to exercise jurisdiction of cybercriminal offences established in their national cybersecurity legislation where one, or more Member States are already conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, shall without prejudice to norms of general international law, consult one another with a view to coordinating their actions on such exercises of jurisdiction.

PART VI- CYBERSECURITY COOPERATION

Cooperation and Mutual Legal Assistance

35.(1) Member States shall coordinate appropriate policies for cybersecurity information sharing amongst relevant security sectors to increase the volume, timeliness, and quality of cyber threat information sharing for States to better protect and defend themselves against cyber threats.

(2) Member States shall coordinate appropriate policies to enhance voluntary information sharing programmes between government, public and private sectors which will enhance classified cyber threat and technical information sharing for law enforcement and stakeholders that provide cybersecurity services.

Measures to Enhance Law Enforcement Cooperation

36.(1) Member States may take appropriate measures to ensure law enforcement cooperation. States shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat cyber-criminal offences covered under their national cybersecurity legislation. Member states shall in particular, adopt effective measures:

(a) to enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered under their national cybersecurity;

(b) to cooperate with other states in conducting inquiries with respect to offences covered under their national cybersecurity legislation: (i) the identity, whereabouts and activities of persons suspected of involvement in such offences

or the location of other persons concerned; (ii) the movement of proceeds of crime or property derived from the commission of such offences; (iii) the movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(c) to provide, when appropriate, necessary information for analytical or investigative purposes;

(d) to facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States concerned;

(e) to exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered under their national cybersecurity legislation.

(2). With a view to addressing cybersecurity in the regions, Member States may consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them to consider cybersecurity objectives.

International Cooperation

37.(1) The operation of domestic cybersecurity legislation shall occur in conjunction to, and with consideration of provisions established by international agreements and mechanisms.

(2) Member States must establish regimes to provide mechanisms to ensure a single point of contact for incidents and their resolution in international cooperation with other governmental, law enforcement and sectoral efforts.

(3) Member States shall make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber

security, and stimulating dialogue between stakeholders. These means may be international, regional, intergovernmental or based on private and public partnerships.

Public -Private Partnership

38.(1) Member States shall develop multistakeholder engagement models for public-private partnership for cybersecurity monitoring, prevention and mitigation and to enhance cyber resilience and trust in the region.

(2) In furtherance of public-private partnership, Member States may establish cyber-security standards for private sector relevant to security and welfare, including establishing monitoring and implementation agencies such as a national cybersecurity committee to administer the implementation of such partnerships.

.

PART VII- CYBERSECURITY MANAGEMENT

Critical Infrastructure

39.(1) Member States shall ensure that national cybersecurity legislation impose strict obligations for the maintenance and protection of computer networks capable of significant disruption, destruction, and interference to critical infrastructure and information systems.

(2) Member States shall identify critical infrastructure at greatest risk of cyber threats.

(3) Member States shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic and financial security, or national security.

(4) Each Member State shall ensure that the national cybersecurity legislation lists and defines what will be considered as 'critical infrastructure' and provide a regulatory framework for the maintenance and protection of 'critical infrastructure'

Computer Emergency Response

40.(1) Member States shall establish specialised cybersecurity management bodies and teams responsible for cybersecurity management and formulate emergency response plans.

(2) Member States may also direct the establishment of national and sectoral teams for the purposes of responding to computer network emergency incidents and coordinate such responses along national, and or sectoral lines. The national and sectoral teams will work in coordination, to respond to, and mitigate cyber incidents and threats.

(3) Member States may mandate the national and sectoral emergency response teams to establish cyber incident registry or database in their respective jurisdictions for the collection and collation of cybersecurity incidents, analysing cyber incidents, and performing cybersecurity supervisory functions.

Cybersecurity Points of Contact

41.(1) To ensure expedited operational cooperation on cybersecurity in the region, Member States shall take appropriate measures to designate an equipped point of contact with trained personnel to facilitate the operation of the network available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning offences established as cyber-criminal offences in national legislation, or for the

collection of electronic evidence necessary for investigative or law enforcement purposes

Cybersecurity Strategies and Framework

42.(1) Member States shall design and develop appropriate cybersecurity strategies and framework to identify, assess, monitor, prevent and mitigate cyberthreats in their various jurisdictions.

(2) The cybersecurity strategy and framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber threats in the jurisdiction.

(3) The cybersecurity strategy shall incorporate international and regional consensus standards and best practices. The cybersecurity strategy shall focus on identifying cross-sector security standards and guidelines applicable to cybersecurity.

(4) The cybersecurity strategy will also identify areas for improvement to enable technical innovation, the monitoring and measuring of organizational standards and provide guidance that enables national cybersecurity sectors to advance services that meet the standards, methodologies, procedures, and processes developed to address cyber threats.

Establishment of a Central Authority for Cybersecurity Regulation

43.Member States shall ensure that the national cybersecurity legislation includes provisions establishing the authority or authorities responsible for regulation of cybersecurity measures in the country, as well as its scope and powers. The National Cybersecurity Authority shall:

a) Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices and breaches with the potential to affect the domestic cyberspace.
b) Perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents
c) Interact with and support state departments responding to cybersecurity.
d) Promote communication across cybersecurity related sectors and departments regarding cybersecurity.
e) Advise the national institutions, bodies, offices and agencies of the Member States on cybersecurity research needs and priorities to support effective responses to current and emerging risks and cyber threats,
f) Oversee the development of a regulatory cybersecurity response guidance to assist state in the continued mitigation of cyber threats.
g) Support the States with implementation of national cybersecurity laws, policies and strategies and assist with the implementation efforts related to the ratification and adoption of regional and international cybersecurity treaties
h) Engage with national and international stakeholders on efforts to manage and evaluate cybersecurity.
i) Raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users, organisations and businesses, including cyber-hygiene and cyber-literacy

Cybersecurity Assistance and Support for Victims

44.(1) In fulfilment of their obligation to monitor and prevent cybersecurity threats and oversee the welfare of citizen, Member States may implement support systems to advise, support and protect the victims of offences established under the national cybersecurity legislation, including

establishing designated agencies which will be charged with the responsibility of victims support

(2) Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by the national cybersecurity legislation, in particular in cases of threat of retaliation or intimidation and having particular regard to the more vulnerable groups of society

(3) Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by the national cybersecurity legislation.

(4) Each State Party shall, subject to its national cybersecurity law, enable views and concerns of victims to be presented and considered at appropriate stages of the criminal proceedings against offenders in a manner not prejudicial to the rights of the defence and consistent with the protection of their rights under the law.

Education and Training

45.(1) Member States are reminded that cybersecurity regimes impose important duties for the maintenance and protection of systems upon governments, private sector, institutions and citizens, therefore, the importance of public education and awareness shall be considered alongside the important function of regulation.

(2) Each State shall adopt measures to develop capacity building with a view to offering training which covers all areas of cybersecurity to different stakeholders.

(3) Member States shall promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization

of professional qualifications as well as development and needs-based distribution of educational material.

(4) As part of the plan for promotion of public education and training, Member States may adopt the following measures: elaborate and implement programmes and initiatives for sensitization, education and training, and dissemination of information on cybersecurity for citizens; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national curricular programme for schools, youths and children.

(5) Member States in fulfilment of their obligation to monitor and prevent cybersecurity threats and oversee the welfare of citizens may implement support systems to advise the vulnerable groups of society on cybersecurity matters

Cybersecurity Research and Development

46.(1) Member States shall support research and development programs to guide the overall direction of national cybersecurity and development for information technology and networking systems to meet the objectives of cybersecurity such as;

a) how to design and build complex software-intensive systems that are relevant for promoting cybersecurity;

b) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

c) how to locally develop and design cybersecurity solution;

d) how to advance solutions that protect critical national infrastructure;

e) how to support privacy in conjunction with improved security; including individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

f) how to address the problem of insider or external cyber threats;

g) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

h) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services;

i) any additional objectives and with input from stakeholders, including appropriate national laboratories, industry, and academia, as appropriate.

Amendments to Domestic Legislation

47.(1) Member States shall also adopt such measures as may be necessary to facilitate appropriate review and amendment of cybersecurity laws to facilitate flexible redress of existing and future cyber threats.

1/11/2022