

# **Standard Operating Procedures for Investigation and Prosecution of Cybercrimes and related Offences**

**FEBRUARY, 2025**

## TABLE OF CONTENT

<b>FOREWORD .....</b>	<b>iii</b>
<b>ACKNOWLEDGEMENT .....</b>	<b>vi</b>
<b>ABBREVIATIONS .....</b>	<b>vii</b>
<b>DEFINITION OF TERMS.....</b>	<b>ix</b>
<b>PART I.....</b>	<b>1</b>
1.1 <i>INTRODUCTION.....</i>	1
1.2 <i>OVERVIEW.....</i>	1
1.2.1 Scope and application .....	4
1.2.2 Objectives of the SOPs .....	4
1.2.3 Document Structure.....	5
<b>PART II.....</b>	<b>6</b>
<b>INVESTIGATION .....</b>	<b>6</b>
2.0 <i>Introduction .....</i>	6
2.1 <i>Crime Reporting .....</i>	12
2.2 <i>Gathering Information.....</i>	12
2.3 <i>Investigation Plan.....</i>	13
2.4 <i>Execution of the Investigation Plan.....</i>	13
2.5 <i>Procedures.....</i>	14
2.5.1 Securing and evaluating the crime scene .....	14
2.5.2 Search and Seizure .....	15
2.6 <i>Chain of Custody.....</i>	21
2.6.1 Documentation .....	23
2.6.2 Packaging .....	23
2.6.3 Labelling.....	24

2.6.4 Transportation .....	24
2.6.5 Storing Electronic Devices.....	24
<b>2.7 Interview.....</b>	<b>25</b>
<b>2.8 Forensic Examination.....</b>	<b>26</b>
<b>2.9 Mutual Legal Assistance and Extradition Request ...</b>	<b>26</b>
<b>2.10 Asset Forfeiture and Recovery.....</b>	<b>27</b>
<b>2.11 Witness Protection .....</b>	<b>27</b>
<b>2.12 Submission of Case File.....</b>	<b>27</b>
<b>PART III.....</b>	<b>28</b>
<b>PROSECUTION.....</b>	<b>28</b>
3.1 <i>Pre-Trial Stage .....</i>	28
3.2 <i>Trial Stage.....</i>	30
3.3 <i>Plea bargaining.....</i>	34
<b>PART IV .....</b>	<b>35</b>
<b>4.0 NON-COMPLIANCE WITH SOPs .....</b>	<b>35</b>
<b>5.0 COMMENCEMENT.....</b>	<b>36</b>
<b>LIST OF ANNEXTURES .....</b>	<b>37</b>
<i>ANNEXTURE 1: INVESTIGATION PLAN.....</i>	37
<i>ANNEXTURE 2: PROSECUTION PLAN TEMPLATE .....</i>	39
<i>ANNEXTURE 3: OFFENCES, ELEMENTS TO PROVE AND MODEL CHARGES .....</i>	40

## **FOREWORD**

The advancement in Information and Communication Technology (ICT) has affected virtually every aspect of the way we live and conduct our daily lives. While these technologies have been a source of development and enabled social and economic progress around our country and the world at large, hardly a day goes by without news of yet another cyber-attack, or the use of ICT in the commission of crime. The National Prosecutions Service (NPS) is aware of these risks posed by the use of ICT in the commission of crimes, which is often transnational and organised in nature and perpetrated in a sophisticated manner. However, the investigation and prosecutions of cybercrimes in Tanzania has faced challenges of inadequate expertise and skills in the collection, preservation, analysis of evidence and proper prosecution of cybercrimes. These challenges led to different investigation and prosecution outcomes for lack of uniformity. Therefore, successful investigation, prosecution and recovery of the proceeds of cybercrimes remain as a complex task which requires special skills and techniques.

On that basis these Standard Operating Procedures (SOPs) sets the uniform standard that will be used in coordination of investigation and prosecution for

effective implementation and enforcement of the cyber laws to address cybercrimes challenges. To do so, investigators and Prosecutors need to develop competences for preventing, investigating and prosecuting cybercrimes and cyber related offences through capacity building on aspect of collection and management of evidence that can be used in prosecutions of individuals and/or corporates who involved themselves in commission of these crimes. That's the primary objective of these SOPs.

It is in this regard, the NPS, has developed the inaugural of SOPs for Investigation and Prosecution of Cybercrimes and related Offences, which includes standard inter-agency procedures and international cooperation aspects. These SOPs will lay out a one-stop-shop for practical guidance in investigating and prosecuting cybercrimes in all its manifestation using sectorial and ancillary legislations. I wish to commend all stakeholders involved in the fight against cybercrimes in Tanzania to use these SOPs to fight against this scourge. Furthermore, the NPS assures all stakeholders that it will oversee the implementation of these SOPs in the fight against cybercrimes in Tanzania.

These SOPs are internal directives intended to guide investigators and prosecutors in dealing with cybercrimes and other related offences.

Sylvester Anthony Mwakitalu  
**DIRECTOR OF PUBLIC PROSECUTIONS**

## **ACKNOWLEDGEMENT**

On behalf of the NPS, I wish to thank the NPS Management, under the stewardship of the Director of Public Prosecutions, Mr Sylvester Anthony Mwakitalu, for their guidance and contribution to develop these Standard Operating Procedures.

The NPS extends immense gratitude to the Ministry of Information, Communication and Information Technology, for its partnership with NPS and support in developing these SOPs.

I am deeply gladdened by the NPS Technical Team for their tireless dedication, commitment and sharing of their knowledge and expertise towards development of these SOPs despite their busy schedules. My appreciations are extended to the Ministry of Constitutional and Legal Affairs, Tanzania Police Force, Prevention and Combating of Corruption Bureau, and Drug Control and Enforcement Authority, for their cooperation in the validation of these SOPs.

Finally, I would like to express my heartfelt gratitude to whoever contributed in development of these SOPs.

Bibiana Joseph Kileo  
**DEPUTY DIRECTOR OF PUBLIC PROSECUTIONS**

## ABBREVIATIONS

CD	Compact Disc
CPA	Criminal Procedure Act
CCTV	Closed-Circuit Television
CMIS	Case Management Information System
DPO	District Prosecutions Officer
DPP	Director of Public Prosecutions
DVD	Digital Versatile Disk
EOCCA	Economic and Organised Crime Control Act
ETA	Electronic Transaction Act
FCU	Financial Crimes Unit
FIU	Financial Intelligence Unit
GPS	Global Positioning System
ICCID	Integrated Circuit Card Identifier
ICT	Information and Communication Technology
IMEI	International Mobile Equipment
IP	Internet Protocol
IR	Investigation Reference
MAC	Media access Control
MLA	Mutual Legal Assistance
NPS	National Prosecutions Service
NPSA	National Prosecutions Service Act
PCCB	Prevention and Combating of Corruption Bureau

PFASA	Police Force and Auxiliary Services Act
PGI	Prosecution General Instructions for State Attorneys and Prosecutors
PGO	Police General Orders
POS	Point of Sale
RPO	Regional Prosecutions Officer
SIM	Subscriber Identity Module
SOPs	Standard Operating Procedures
TCRA	Tanzania Communications Regulatory Authority
TPF	Tanzania Police Force
TEA	The Evidence Act
USB	Universal Serial Bus
WiFi	Wireless Fidelity
VPN	Virtual Private Network

## **DEFINITION OF TERMS**

For the purpose of these SOPs, the following terms shall have the following meaning:

Authorized officer	Has the meaning ascribed to it under Section 3 of the Economic Offences Specification of Offences for Consent, Notice, 2021;
Assignee	Means a Prosecutor to whom an assignment is given;
Central Authority	Means the DPP of URT under Mutual Assistance in Criminal Matters Act or Minister responsible for Legal Affairs under Extradition Act.
Closed-Circuit Television	Means a television system in which video signals are transmitted from one or more cameras by cable to a set of monitors, used especially for security purposes;
Criminal racket	Has the meaning ascribed to it under Section 3 of EOCCA
Global Positioning	Means an accurate worldwide navigational; and surveying facility based on

System	the reception of signals from an array of orbiting satellites;
Faraday bag	Means an enclosed and sealed tool which prevents signals from being sent and received to avoid cyber-attack or tampering with evidence from the digital device;
First responder	Means a Law enforcement Officer who is among those responsible for receiving complaints, going immediately to the scene of crime or emergency to provide assistance;
Integrated Circuit Card Identification number	Means a unique identifier for circuit cards, such as Subscriber Identity Module cards and credit cards;
Internet	Means a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols;
Investigator	Means any officer acting in an investigative role;
Law	As defined under Cybercrime Act

enforcement Officer	as amended
Organized crime	Has the meaning ascribed to it under Section 3 of EOCCA;
Officer	Means any person acting on behalf of the DPP;
Password	Means a string of characters or secret words or phrase that must be keyed to gain access to a computer, network, service, to a smart phone or similar device;
Prosecutor	Means a public prosecutor as defined under Section 3 of NPSA;
Router	Means a device that forwards data packets to the appropriate parts of a computer network;
Supervisor	Means Director of Public Prosecution, Regional Prosecutions Officer or District Prosecutions Officer;
Tainted properties	Has the meaning ascribed to it under Section 3 the Proceeds of Crimes Act;

## PART I

### 1.1 INTRODUCTION

### 1.2 OVERVIEW

Cybercrimes pose significant challenges to society that affect the security and economy. Although much is being done, in law, policy and practice, to address these challenges, adequate measures remain difficult to conceive and implement, as the field is dynamic, complex, and global. The Standard Operating Procedures are designed to provide baseline for investigations and prosecutions of cybercrimes and related offences. Thus, SOPs can address the diversity in prosecution and investigation of cybercrimes by addressing all aspects that investigator and prosecutor need to follow when dealing with cybercrimes and related offences. These SOPs, acts as a bridge in addressing the challenges that existed before its inaugural.

These SOPs are aimed at capacity building among prosecutors and investigators in order to combat cybercrimes and related offences. The SOPs to investigators intends to acquaint them with knowledge and techniques to investigate cybercrimes and related offences in an effective, efficient, fair and forensically sound manner. The

prosecutors, on the other hand, are responsible for coordinating the investigation, making sure that the procedures and, principles of collecting and managing the evidence are well observed. Also, prosecutors while discharging their duties are mandated to make decisions to charge, institute criminal proceedings, present evidence in court, and execution of court orders timely.

Hence, investigators and prosecutors need to work on structured and documented operational procedures that are standardized in accordance with the laws governing investigation and prosecution of Cybercrimes and ensure compliance which reflects best practices.

Conversely, the laws governing Cybercrimes in Tanzania includes Cybercrimes Act, The Evidence Act, The Electronic and Postal Communications Act and the Electronic Transactions Act which lay down procedures for investigation, collection of evidence, use of electronic evidence, legal recognition of electronic transactions, the use of information and communication technology, and admissibility of Electronic Evidence. However, the investigation and prosecution of cybercrimes in Tanzania has faced challenges of inadequate expertise and skills in the identification, collection,

preservation, analysis of evidence and proper prosecutions of cybercrime offences. These challenges led to different investigation and prosecution outcomes for lack of uniformity among the investigators and prosecutors. Despite having the laws in place that lay down procedures in dealing with cybercrimes, there is no internal single document which provide for guidance to investigators and prosecutors in implementing these laws and overcoming the challenges in identification, collection, storing, preservation and tendering of electronic evidence.

Therefore, due to this deficiency, the DPP has introduced these SOPs which are intended to lay down and maintain a consistent and standardized approach for investigation and prosecution of cybercrimes and related offences across the country. They are instructive guidance to investigators and prosecutors on what they should do, at minimum, while dealing with cybercrimes and related offences. The intention is to reduce, if not to avoid, mistakes which are invariably committed during investigation and prosecution of cybercrimes.

The SOPs are not merely a bold statement but rather, working tool. It is against this backdrop, the DPP in terms of Section 18(1) and 24(2) of the

National Prosecutions Service Act, Cap. 430 has issued these SOPs to guide investigators and prosecutors in investigation and prosecution of Cybercrimes and related offences.

### **1.2.1 Scope and application**

These SOPs are internal administrative directives intending to guide Prosecutors and Investigators in the course of investigation and prosecution of Cybercrimes and related offences. Nothing in these SOPs is intended to alter any legal procedure established by Legislations in handling cybercrimes and related offences. Thus, they do not affect any rule of law or procedure relating to the admissibility of evidence in Courts of Law.

### **1.2.2 Objectives of the SOPs**

The Objectives of these SOPs are;

- a) To provide uniform standards of handling investigation and prosecution of Cybercrimes and related offences.
- b) To enhance and strengthen coordination of investigation and the effective enforcement of the cybercrime laws by building capacity of investigators and prosecutors.
- c) To assist the investigators in the process of collecting, preserving, analysing and storing of evidence by following established forensic principles and best practices.

d) To ensure that electronic evidence is identified timely and properly collected, stored, preserved and presented in court in line with the established procedures.

### **1.2.3 Document Structure**

These SOPs are comprised of four main parts; Part I, II, III, and IV. Part I is an overview of the SOPs, scope and application and objectives. Part II provides for investigation guidance. Part III covers prosecution of cybercrimes and related offences. Part IV addresses the legal status of the SOPs and the consequences of non-compliance.

## PART II

### INVESTIGATION

#### 2.0 Introduction

The goal of cybercrime investigation is achieved by identifying how the crime was committed, evidence was gathered and preserved to ensure its admissibility in court. Considering volatile nature of digital evidence, necessary investigation steps should be taken as early as possible depending on the circumstances of each case once the crime is reported.

Prosecutors and investigators need to be acquainted with the knowledge of digital devices as potential source of evidence such as finger print and all the information stored. Some of these digital devices are described in the table below;

	Device	Photo	Potential Evidence
1.	Desktop Computer/Laptop		<ul style="list-style-type: none"><li>• The device itself may be evidence.</li><li>• The device may contain digital evidence in files and folders stored including deleted files and other hidden information.</li></ul>

			<ul style="list-style-type: none"> <li>• Network Configurations and connections</li> <li>• Registry History i.e. executed programs and USB connectivity History</li> <li>• Browser history.</li> </ul>
2.	Monitor		<p>All the graphics and files that are opened and visible on the screen in switched-on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and, through the description in the seizure certificate</p>
3.	Digital Camera		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Images, videos, sound, time and date stamps</li> </ul>

4.	Hard Disk		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• All the information stored</li> </ul>
5.	Mobile Phones		<ul style="list-style-type: none"> <li>• SMS</li> <li>• WhatsApp</li> <li>• Call Logs</li> <li>• Geo-location</li> <li>• Emails</li> <li>• Documents</li> <li>• Videos</li> <li>• Pictures</li> <li>• Audios</li> <li>• Instant Messaging</li> <li>• Browsing History</li> </ul>
6.	Portable devices		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• File and information stored</li> <li>• Deleted files</li> </ul>

7.	Digital Watch		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Information like, address book, notes, appointments, cameras, emails, phone numbers, messages, location, call logs etc.</li> </ul>
8.	Global Positioning System		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Travelling logs, location, way point coordinates, way point name, date and time etc.</li> </ul>
9.	Smart Cards and Biometric Scanner		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Identification/authentication information of the card and the user, level of access, configuration and permission</li> </ul>

10.	Credit Card Skimmers		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Tracks of magnetic stripes contain cardholder's information which may include I card expiration date, I users address, I card numbers, I users name</li> </ul>
11.	CDs and DVDs		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Files/data</li> </ul>
12.	Printer		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Data like number of prints last printed and some maintain usage logs, time and date information. If attached to a network, they may store network identity information. In addition it can also be examined for finger print</li> </ul>

13.	Scanner		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Data/information stored</li> </ul>
14.	Telephone		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Contact list, messages (text and voice), memos, password, and phone numbers and call identification information.</li> <li>• Appointment information</li> <li>• voice note</li> </ul>
15.	CCTV Camera		<ul style="list-style-type: none"> <li>• Device itself</li> <li>• Footage, location, date and time</li> </ul>
16.	Other Devices		<ul style="list-style-type: none"> <li>• May contain crucial information</li> </ul>

## **2.1 Crime Reporting**

Upon receipt of complaint, the officer receiving shall immediately do the following;

- (a) Make an initial assessment of the report on the nature and seriousness of the crime.
- (b) Inform cybercrime Desk for the purpose of securing the evidence.

## **2.2 Gathering Information**

Investigators shall gather information that will help them to prepare, plan and develop a general methodology on how the investigation will be conducted. Nature of crime under investigation will determine necessary equipment for the exercise and the preparation of the most appropriate technical procedures for each case. Therefore, in gathering necessary information, the investigator shall do the following;

- a. Analyse the information on how the cybercrime was committed,
- b. Identify the tools and techniques used to commit the crime,
- c. Identify the crime scene,
- d. Identify the suspects,
- e. Identify the victim,
- f. Identify items to be seized,

- g. Preserve and store of the seized evidence,
- h. Identify relevant laws to guide investigation,
- i. Identify relevant evidence required to prove an offence and
- j. Identify protection needs for the victims and potential witnesses.

### **2.3 Investigation Plan**

Considering the volatile nature of the electronic evidence, it is important to establish a clear plan to identify digital evidence, secure it and conduct such investigation properly. The investigator shall, after gathering initial information and forming an opinion that the crime has been committed, proceed to prepare an investigation plan in accordance with the investigation plan template (ANNEXTURE 1).

### **2.4 Execution of the Investigation Plan**

In execution of the Investigation Plan together with other investigation measures, the investigator shall do or cause the following to be done;

- a. Communicate with stakeholders/service providers if necessary,

- b. Obtain a search order or search warrant as the case may be,
- c. Ascertain the assets connected with the offence for the purpose conducting financial investigation,
- d. Attend and examine the crime scene and,
- e. Liaise with the RPO or DPO for coordination.

## **2.5 Procedures**

Digital evidence is fragile by its nature, thus for the evidence to be admissible in court, the laws require it to be authentic. Therefore, proper procedures must be adhered to make sure evidence is not altered or modified during the investigation. This section covers the proper procedures to be observed by investigators during the investigation of digitally generated evidence.

### **2.5.1 Securing and evaluating the crime scene**

At the crime scene the Investigator shall do the following;

- a. Prevent unauthorized access to the evidence and perimeters,
- b. Allow any printers to finish printing,

- c. Inspect for the existence of wireless connections,
- d. Document the crime scene by taking a Photograph/video of the scene before, during and after the search, or
- e. Draw a sketch plan of the scene and label the ports and cables if the camera is not available,
- f. Identify digital device(s),
- g. Identify where digital evidence is located,
- h. Identify evidence by level of volatility,
- i. Know how the evidence stored is vital to determine which process is to be employed to facilitate its recovery,
- j. Conduct preliminary interview with the victim, suspect and witnesses,
- k. If the device is **ON**, take closer photographs to capture date, time and opened files.

### **2.5.2 Search and Seizure**

Search can be conducted to persons, premises, vehicles, computer system and other places. Seizure of digital devices is important part of the duties of the Investigator and therefore they must be planned and undertaken in a systematic and professional manner. Failure to do so

will result into evidence being rendered inadmissible. Search and Seizure must be conducted without prejudice to the provisions of Section 31 of Cybercrimes Act, Section 38, 40 and 42 of the Criminal Procedure Act and other SOPs for forensic examinations.

The following are the general procedures to be adhered to when attending a crime scene in which computers or electronic technologies are involved;

#### **A. Search and Seizure of Desktop Computer or Laptop when “POWERED OFF”;**

- i. Do not turn it “ON”, leave it “OFF”. The investigator shall not make any attempt to search a computer for evidence,
- ii. Photograph the back and front of a computer, its location and any media devices attached to it prior to moving any evidence,
- iii. Confirm if the computer is switched “OFF” by moving the mouse,
- iv. Document connectivity,
- v. Disconnect and label cables,
- vi. Seize any power cables and manuals for future use,
- vii. Confirm the presence of the hard drive if the hard drive is present, document unique

identities, i.e. Make and Model and no hard drive is present, inform the team.

## **B. Search and Seizure of Desktop Computer or Laptop when “POWERED ON”;**

- (i) Observe the order of volatility,
- (ii) Do not touch the keyboard or mouse,
- (iii) Do not use the computer or attempt to search for evidence,
- (iv) Observe what is displayed on the screen and record it by taking a photograph of the screen to capture opened files, running programs, date and time,
- (v) If the screen displays valuable evidence (instant messages, emails or open files), an investigator shall seek advice from a forensic expert on how to collect volatile data as they may get lost when the computer system is shut down,
- (vi) If encryption exists, collect logical copies,
- (vii) Disable network connectivity,
- (viii) Disconnect from power by pulling the plug on the computer itself, and in the case of a laptop remove the battery,
- (ix) Do not use the normal “**SHUTDOWN**” procedures as it will make changes to the

- stored data or may initiate wiping software to run if installed,
- (x) If it is a laptop and the battery is not removable shut down the computer by pressing the power button,
  - (xi) Disconnect all devices from the computer,
  - (xii) Seize and pack all evidence,
  - (xiii) Document all the steps involved in seizure of electronic evidence,
  - (xiv) Search for notebooks, diaries or any paper documents which may contain any valuable information (username and passwords) that may be useful in future,
  - (xv) For specific procedures, the examiner shall adhere to the Agency's procedures for specific devices as documented on their SOPs.

### **C. General procedures for seizing Mobile phones and other Digital Devices;**

- (i) If the device appears to be “OFF”, leave it “OFF”.
- (ii) If the device appears to be “ON”, do not interrupt it, (i.e. do not be tempted to have a quick look by using touchscreen or keypad) other than switch it “OFF” – if the off switch is obvious,

- (iii) Note down the exact time and location where the switching off occurs and make this available to whoever will examine the device,
- (iv) Note down the condition and state of the device when seized,
- (v) Identify and collect any associated power supplies or other external accessories for the device. Original power supply cables are particularly important as sometimes may be needed for examination,
- (vi) If possible, isolate the device from the networks by using a Faraday bag, Faraday cage or other radio-frequency shielded container. Be aware that devices which are “ON” may run their batteries down more quickly once shielded from communication networks,
- (vii) Record any unique identifying marks or distinguishing characters (i.e Serial Numbers, IMEI, license stickers, any damage etc.),
- (viii) Pack the device(s) and associated cables in tamper-evidence packaging materials. Complete continuity labels and enter details into the device log. Ensure that any associate external power supplies and

devices are packaged with the device if possible and ensure that identifying marks are visible through the package.

#### **D. E-mails and Social media accounts**

- (i) If it's social media accounts and other public domain accounts such as Gmail, Yahoo, iCloud, seize the account by obtaining the credentials (username and password) from the owner. Disable all recovery options and change the password. If an e-mail message is involved, the Investigator should collect e-mail header information,
- (ii) The investigator shall issue an order to any person having control over computer system to disclose any data stored in the said computer system or device for the purpose of investigation,
- (iii) The investigator shall issue an order to any person having control over computer system to preserve data of his computer for a period not exceeding fourteen (14) days as per provisions of Section 31(i)(a) & (b) of the Cybercrimes Act, where such data is vulnerable to loss or modifications,
- (iv) Where a period exceeds fourteen (14) days the Investigator shall make application to

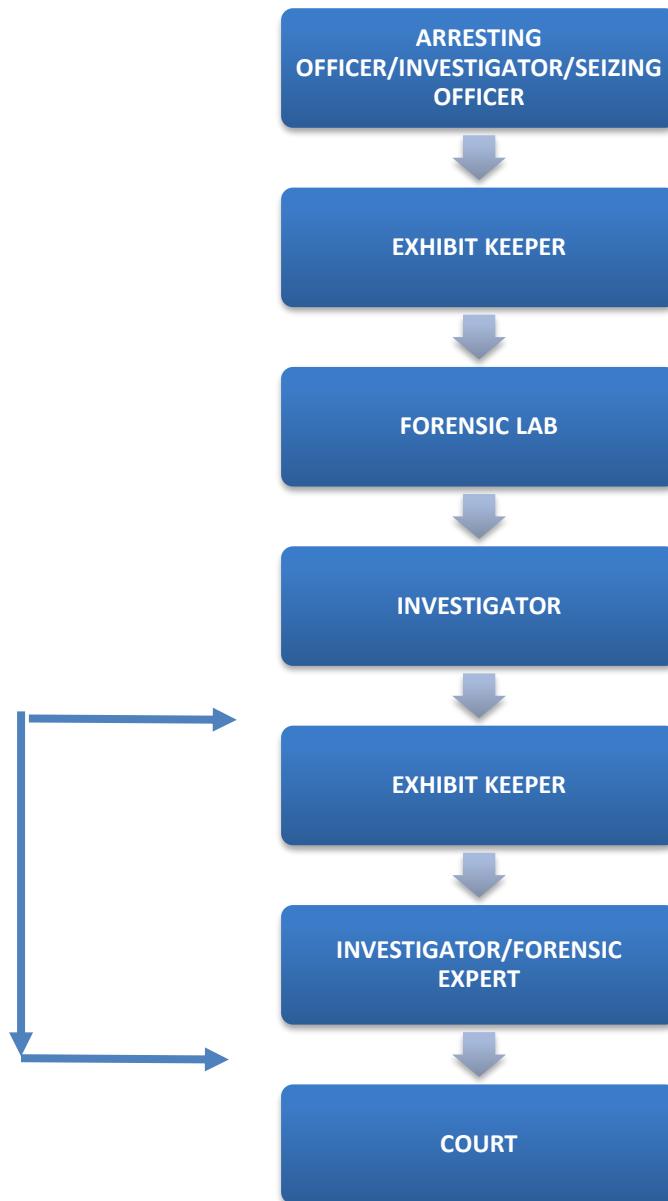
Court to extend the period subject to the provisions of Section 37(7) of the Cybercrimes Act,

- (v) Where the computer system is rendered inaccessible during the search or seizure, the officer shall prepare a list of seized items and those rendered inaccessible,
- (vi) If the suspect denies disclosure of data deliberately, the investigator shall liaise with the DPO or RPO for *ex parte* order as per Sections 36 and 38 of the Cybercrimes Act.

## **2.6 Chain of Custody**

Chain of custody of digital devices shall be maintained from the time they are seized up to when they are presented in court as evidence. In maintaining the chain of custody, the investigator shall ensure proper chronological documentation and/or paper trail, showing the seizure, custody, control, transfer, analysis and disposition of evidence, be it physical or electronic.

# PICTORIAL PRESENTATION OF CHAIN OF CUSTODY



### **2.6.1 Documentation**

Take photographs and or video prior, during and after search;

- a. Mark and label properly all item(s) seized,
- b. Fill all relevant documentations such as certificate of seizure, chain of custody, activities log (investigation diary),
- c. Make a brief summary report of search and seizure, including remarks if any,
- d. Issue a copy of list of items seized to a person from whom the items have been seized;

### **2.6.2 Packaging**

- a. Ensure that all evidence has been properly documented, packaged, and labelled,
- b. Use packaging materials such as bubble wrap,
- c. Prevent accidental booting by placing evidence tape over disk drives and power outlet,

### **2.6.3 Labelling**

The collected digital evidence shall be properly;

- a. Numbered,
- b. Labelled and
- c. Tagged to contain relevant details of the investigation report.

### **2.6.4 Transportation**

When the device is transported from one place to another, the Investigator shall;

- a. Ensure safety,
- b. Maintain chain of custody and reduce it to a few people as possible without missing the required standard.

### **2.6.5 Storing Electronic Devices**

- a. Electronic devices should be stored in a climate-controlled area to prevent its exposure to water, moisture and heat,
- b. The area should be secure and away from dust and magnetic devices.

## **2.7 Interview**

### **a. On-Scene Interview**

The Investigator shall make an oral interview with the witnesses and suspects at the scene of crime to gather the information that will assist forensic examiner at the later stage of examination. The question may be for establishing length of ownership of the seized devices, users of the seized devices, email account, login names and passwords, existence offsite storage or hidden storage devices, internet service providers and ant-forensic measures.

### **b. Post Arrest Interview**

After the suspect has been arrested and kept in custody, the investigator shall cause the suspect to be interviewed in accordance to the relevant law governing interview of suspects.

### **c. Interview of Victims and Witnesses**

During investigation, the investigator shall cause interview to be done to victims/witnesses for purposes of collecting necessary information.

### **d. The interview conducted shall be reduced into writing in accordance with the law governing interview of witnesses.**

### **e. Where the offence involves a corporate or institution, among of the witnesses to be interviewed include custodians and users.**

## **2.8 Forensic Examination**

- a) All digital forensic examinations must be initiated by formal requests from investigating organs.
- b) A request for digital forensic examination shall be submitted with a Forensic Laboratory Request Form if any.
- c) Contain Investigation Reference (IR) Number and offence, list of digital devices to be examined, scope of examination.
- d) Forensic examination shall be conducted by a trained examiner possessing qualifications as per Section 205A and 205B of the Criminal Procedure Act.
- e) Upon completion of forensic examination, the Cyber Forensic Expert shall prepare a Report and resubmit it to the requesting Organ together with the electronic devices examined.

## **2.9 Mutual Legal Assistance and Extradition Request**

The Investigative Organ when conducting investigation and become aware that some of evidence or the suspect(s) are located outside the United Republic of Tanzania, shall liaise with the Central Authority for Mutual Legal Assistance and Extradition request for coordination and shall adhere to procedures as provided in Guidelines to Prosecutors and Competent Authorities for Making

and Executing Mutual Legal Assistance and Extradition Request of 2023.

## **2.10 Asset Forfeiture and Recovery**

The investigator when conducting investigation and becomes aware that, there are assets connected with the offence, shall conduct financial investigation for the purpose of identifying and tracing assets in compliance with the procedures provided for under Assets Forfeiture, Recovery and Management Guidelines, 2023.

## **2.11 Witness Protection**

The investigator when conducting investigation and becomes aware that, there is a witness who is in danger and or in threat and needs protection shall communicate with RPO or DPO for witness protection measures as per Witness Protection Guidelines, 2023.

## **2.12 Submission of Case File**

After completion of investigation, the investigator shall submit the case file to DPO, RPO or DPP as the case may be.

## PART III

### PROSECUTION

#### **3.1 Pre-Trial Stage**

- a) Upon receipt of cybercrime investigation case file RPO, DPO or Officer, as the case maybe, shall ensure the same is registered in the NPS Case Management Information System (CMIS) and physical Cybercrime Register,
- b) The RPO, DPO or Officer shall immediately assign the case file to the Prosecutor for review of evidence,
- c) The Assignee shall assess Witness's vulnerability and danger, if needs arise apply for witness protection measures in line with the Witness Care and Protection Guidelines, 2023,
- d) In deciding whether to charge or not, the Assignee shall be guided by the principles enshrined in the Guidelines on the Decision to Charge and Related Matters, 2023,
- e) The Assignee, basing on the evidence collected, shall ascertain if the chain of custody, reliability, authenticity and

integrity of exhibit(s) collected has been preserved and maintained,

- f) When the Assignee forms an opinion that there are assets involved on the matter, shall adhere to the procedures provided in the Asset Forfeiture, Recovery and Management Guidelines; When the Assignee becomes aware that there is evidence or suspect located outside of the United Republic of Tanzania, shall comply with the conditions set out in the Guidelines to Prosecutors and Competent Authorities for Making and Executing Mutual Legal Assistance and Extradition Request,
- g) The RPO, DPO or Officer after forming an opinion that the evidence collected does not disclose a prosecutable case, shall close or direct further investigation of the cybercrime investigation case file, as the case maybe, in accordance with the procedures outlined under PART III of the Guidelines on the Decision to Charge and Related Matters,
- h) The assignee after being satisfied that the available evidence suffices to charge the suspect(s), shall with supervisor's approval prepare a charge. In preparing a

charge, the prosecutor shall be guided by the Guidelines on the Decision to Charge and Related Matters and templates in **ANNEXTURE 3** and For cybercrime offences which are economic in nature thus requiring consent, the prosecutor shall ensure that consent is issued in accordance with Economic Offences (Specification of Offences for Consent) Notice, GN 496H of 2021,

- i) Where economic case referred in Paragraph (vii) above is instituted in the Court Subordinate to the High Court, the Prosecutor shall ensure that the certificate conferring jurisdiction is obtained,
- j) The RPO, DPO or Officer shall ensure that Consent and Certificate referred in paragraphs (vii) and (viii) above are accordingly filed and record of the trial court reflects the same, and
- k) The RPO, DPO or Officer shall notify the Investigator in writing on the decision.

## **3.2 Trial Stage**

### **3.2.1 Plea of guilty**

In the event, the accused pleads guilty, the prosecutor shall read over the facts of the case according to the

requirements of Section 228 of the Criminal Procedure Act and tender exhibits depending on the circumstances of the case.

### **3.2.2 Preliminary Hearing**

When the accused pleads not guilty and before the commencement of the hearing of the case, the prosecutor shall ensure the following;

- a. The detailed facts of the case are prepared in compliance with Section 192 of the CPA and Section 35 (1) of EOCCA, PGI and other relevant laws, Regulations and Guidelines,
- b. The prepared facts disclose essential elements of offences and reflect sufficiently the nature of the case based on the evidence available,
- c. The prepared facts are submitted to the Supervisor for vetting/approval,
- d. In court while reading the facts, the accused pleads to the facts in person,
- e. Memorandum of agreed facts is drawn and endorsed by the Magistrate, Prosecutor and Accused together with his Advocate, if any,
- f. Where the case is tried by the Corruption and Economic Crimes Division of the High Court, the defence complies with Rule 15(2) of the Economic and Organized Crime Control (Corruption and Economic Crimes

Division Procedure) Rules GN NO 267 of 2016 by giving names and addresses of their intended witnesses as well as list of exhibits to be relied upon.

### **3.2.3 Hearing of the Case**

During the hearing of the cybercrime case the prosecutor shall ensure the following;

- a. Develop and use a prosecution plan as a guidance tool throughout the trial of the case as per ANNEXTURE 2,
- b. Conduct a meeting with the investigator with a view to brainstorm and strategize on the prosecution case including inspection of exhibits (physical and documentary) intended to be tendered in court and assessing their admissibility status,
- c. To arrange and meet relevant witnesses before hearing for trial preparations; Where exhibit(s) needs to be disposed, the Prosecutor shall apply and obtain necessary orders from the court as per Asset Forfeiture, Recovery and Management Guidelines,
- d. Regular review of the charge along with the presented evidence and suggest amendment, if need be,

- e. Present the evidence (documentary or physical) in court for proving all elements of the offence(s) as provided in ANNEXURE 3,
- f. While presenting the evidence pointed out in paragraph (e) herein above, the Prosecutor shall observe principles of authenticity under Section 18 of Electronic Transaction Act, Cap 442 which are:-

- i. Originality of the data message**

The prosecutor shall lead a witness to lay foundation on how the evidence and its originator were identified and obtained, digital evidence has not been altered or tempered with and the data message is what it purports to be.

- ii. Reliability of the data message**

The prosecutor shall ascertain reliability of the manner in which the data message was generated, stored or communicated and the reliability of the manner in which the integrity of the data message was maintained.

- iii. Relevancy**

The prosecutor shall lead the witnesses to convince the Court that the evidence adduced is relevant to the fact in issue.

#### **iv. Chain of custody**

The prosecutor shall lead the witness in proving that chain of custody of the seized digital evidence is preserved from the time of seizure to the time of presenting the same in court by;

- (aa). Observing nature and expertise of witnesses depending on the roles played during investigation of the cybercrime case,
- (bb). Anticipate and prepare himself for any possible objections and defences that may be raised as well as possible provisions of law and decided cases to be used in countering the anticipated objections and defences.

### **3.3 Plea bargaining**

Whenever there is a request to negotiate a plea agreement under Section 194A of CPA, the prosecutor shall ensure that, the Plea-Bargaining Guidelines, 2022 issued by the DPP are complied with accordingly.

## PART IV

### 4.0 NON-COMPLIANCE WITH SOPs

- A. Without showing good cause or prior written permission in advance from DPP, RPO or RCO, any violation or non-compliance with these SOPs shall be reported to the DPP.
- B. For serious or repeated violations, the DPP may
- . impose at his or her discretion any of the following;
  - i. Issue a directive to obtain information regarding the non-compliance,
  - ii. Issue a directive to an investigator or prosecutor under section 17 of the National Prosecutions Service Act, to take steps to comply with the SOPs provisions,
  - iii. If a Directive issued under wilfully refused or neglected by an investigator or prosecutor, such non-compliance would be deemed to amount to an offence and measures against such offender shall be taken in line with provisions of section 17 of the National Prosecutions Service Act, and
  - iv. Revocation or suspension of prosecution Instrument
- C. Given the DPP's supervisory mandate for all investigations and prosecutions, the DPP may also

recommend to the disciplinary authority of investigator or prosecutor any of the following steps:

- i. Re-allocation of a matter to another investigator or prosecutor,
- ii. Imposition of enhanced supervision in relation to the investigation or prosecution of the matter,
- iii. An informal warning,
- iv. A notice placed on the personnel record of the person in non-compliance,
- v. A requirement for further training or skills development/continued professional development,
- vi. Demotion, and/or
- vii. Termination of employment.

## **5.0 COMMENCEMENT**

These guidelines shall come into operation from the date of signing.

Signed at Dodoma this .....day of February, 2025.

## LIST OF ANNEXTURES

### ANNEXURE 1: INVESTIGATION PLAN

Investigation File Number	
Investigator	
Assignment Date	
Assignor	
Suspect (s)	
Timeline for Investigation	
<b>BRIEF FACTS OF THE ALLEGATIONS</b>	
Offences Disclosed	Element to be proved(refer to element worksheet)

<b>WITNESSES TO BE INTERVIEWED</b>				
Name of Witness	Contact	Location	Position/relationship with the accused	Relevance of evidence

<b>WITNESS PROTECTION</b>				
Name of Witness	Location	Nature/type of threat	Protection Measure	Remarks

<b>EXHIBITS TO BE COLLECTED</b>				
Name of Exhibit	Nature/type of Exhibit	Location	Custodian	Relevance of the Exhibit

<b>INVESTIGATION ACTIONS TAKEN</b>					
Activity	Officer Responsible	Evidence Obtained	Relevance of Evidence	Date of Activity	Remarks

<b>ASSETS INVOLVED</b>					
Name and Particulars of Asset	Owner of Asset	Location/Custody	Value of Asset	Action to be taken	Remarks

<b>MUTUAL LEGAL ASSISTANCE/EXTRADITION</b>			
Evidence/Suspect	Location/Country	Action to be taken	Remarks

Investigation Officer.....

Signature.....

Date.....

## ANNEXTURE 2: PROSECUTION PLAN TEMPLATE

FILE NO:							
COURT:							
CASE NUMBER:							
DATE OF COMMENCEMENT OF TRIAL							
SUPERVISOR:							
INVESTIGATOR(S):							
ASSIGNED PROSECUTOR (S):							
WITNESS (S)	SERIAL ORDER OF TESTIMONY	INGREDIENTS OF OFFENCE	KEY POINTS TO BE PROVED	EXHIBITS TO BE TENDERED	ADMISSIBILITY OF EXHIBITS	ANY POSSIBLE OBJECTION(S) /DEFENCE(S)	REMARKS

## **ANNEXURE 3: OFFENCES, ELEMENTS TO PROVE AND MODEL CHARGES**

### **A.OFFENCES UNDER THE CYBER CRIME ACT NO. 14 OF 2015**

OFFENCE			
S. 4(1) and (2) Illegal access			
Elements	Clarifications	Possible evidence	Witness
<ul style="list-style-type: none"> <li>-Intentionally and Unlawful</li> <li>-access OR cause to be accessed</li> <li>-Through a Computer system</li> </ul>	<p>Computer system, access and device as defined under S. 3</p>	<ul style="list-style-type: none"> <li>-Proof Ownership of the system (custodian)</li> <li>- Login or logout details</li> <li>- List of authorized personnel to the system</li> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of Seizure</li> <li>- Cyber forensic analysis Report</li> </ul>	<ul style="list-style-type: none"> <li>-System Administrator</li> <li>- Service provider</li> <li>-Cyber forensic expert</li> <li>- Officer conducting the search</li> <li>-Independent witness (if any)</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**ILLEGAL ACCESS;** Contrary to Section 4(1) and (2) of the Cybercrimes Act No. 14 of 2015

**PARTICULARS OF OFFENCE**

**XY**, on diverse dates between 3<sup>rd</sup> January, 2020 and 14<sup>th</sup> February, 2020 at Tabata area within Ilala District in the City and Region of Dar es Salaam, did intentionally and unlawfully access a computer system to wit .....(insert name of the computer system e.g. Banking system or computer programme or application or software and the mode of unlawful access).

**OR**

**STATEMENT OF OFFENCE**

**ILLEGAL ACCESS;** Contrary to Section 4(1) and (2) of the Cybercrimes Act No. 14 of 2015

**PARTICULARS OF OFFENCE**

**XY**, on diverse dates between 3<sup>rd</sup> January, 2020 and 14<sup>th</sup> February, 2020 at Tabata area within Ilala District in the City and Region of Dar es Salaam, did intentionally and unlawfully cause a computer system to wit ..... (Insert name of the computer system e.g. Banking system or computer programme or application or software and the modality of the unlawful access) to be accessed by ..... (Insert name of the person who accessed).

OFFENCE			
S. 5(1) and (2) Illegal Remaining			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
<ul style="list-style-type: none"> <li>- Intentionally and unlawfully.</li> <li>- Remain OR continue to use</li> <li>- A computer system</li> <li>- Time which he was allowed to access</li> <li>-The time he remained in the system after expiration he was allowed to access the system</li> </ul>		<ul style="list-style-type: none"> <li>- Proof Ownership of the system (custodian).</li> <li>- Login OR Logout details.</li> <li>- List of authorized personnel to the system.</li> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of Seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Details of the authorization/ Agreement to access the system.</li> <li>- (time frame to access the system, level of access)</li> </ul>	<ul style="list-style-type: none"> <li>- System Administrator</li> <li>- Service provider</li> <li>- Cyber forensic expert</li> <li>- Officer conducting the search</li> <li>- Independent witness (if any)</li> </ul>

## **MODEL CHARGE** **STATEMENT OF OFFENCE**

**ILLEGAL REMAINING;** Contrary to Section 5(1) and (2) of the Cybercrimes Act No. 14 of 2015.

### **PARTICULARS OF OFFENCE**

**ZY**, on diverse dates between 10<sup>th</sup> February, 2022 and 30<sup>th</sup> February, 2022 at Njiro area within Arusha District in Arusha Region, did intentionally and unlawfully continue to use a computer system to wit .....  
(Insert name of the computer system eg Banking system or computer programme or application or software) after the expiry of time which he was allowed to access the computer system.

OFFENCE			
S. 6(1) (a) (b) and (2) Illegal Interception			
ELEMENTS	CLARIFICATIONS	POSSIBLE EVIDENCE	WITNES
<b>A. Interception</b>			
- Intentionally and unlawfully - interception  i)- non-public transmission - to or from - computer system  OR ii)-non-electromagnetic emission - from computer	Interception is as is defined under S. 3	- Login or logout details  - Credentials used to log in  - Device used  - Software used  - Certificate of Seizure	- System Administrator - Owner of the system - Officer conducting the search - independent witness (if any) - Cyber forensic expert

<p>system</p> <p>OR</p> <p>iii)- non-public computer system</p> <ul style="list-style-type: none"> <li>- connected to another computer system</li> </ul>		<ul style="list-style-type: none"> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	
<b>B. Circumventing</b>			
<ul style="list-style-type: none"> <li>- Intentionally and unlawful circumvent</li> <li>- The protection measures implemented to prevent access to the content of non-public transmission</li> </ul>		<ul style="list-style-type: none"> <li>- Access to the system</li> <li>- Logs details</li> <li>- Security measures implemented to prevent access</li> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of Seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic expert</li> <li>- Systems Administrator</li> <li>- Person conducting the search</li> <li>- independent witness (if any)</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**ILLEGAL INTERCEPTION;** Contrary to Section 6(1) (a) of the Cybercrimes Act No. 14 of 2015 read together with Paragraph 36 of the First Schedule to, and Section 57(1) and 60 (2) of the Economic and Organized Crime Control Act [[CAP 200 R.E. 2022]].

**PARTICULARS OF OFFENCE**

**CM**, on diverse dates between 25<sup>th</sup> March, 2019 and 30<sup>th</sup> May, 2020 at Kisasa area within Dodoma District in the Region of Dodoma, did intentionally and unlawfully intercept by (name the mode of interception) to a non-public transmission within a computer system to wit ..... (Insert name of the computer system) by using a technical devise namely ..... (Insert name the technical device e.g. software, computer programme of application).

**OR**

**STATEMENT OF OFFENCE**

**ILLEGAL INTERCEPTION;** Contrary to Section 6(1) (b) of the Cybercrimes Act No. 14 of 2015 read together with paragraph 36 of the First Schedule to, and Section 57(1) and 60 (2) of the Economic and Organized Crime Control Act Cap. 200 R.E. 2022.

## **PARTICULARS OF OFFENCE**

**CM**, on diverse dates between 25<sup>th</sup> March, 2019 and 30<sup>th</sup> May, 2020 at Kisasa area within Dodoma District in the Region of Dodoma, did intentionally and unlawfully circumvent the protection measures to prevent access to the content of non –public transmission by .....(insert name of the act of circumventing e.g. tempering with password, backup data, firewalls, encryptions)

<b>OFFENCE</b>			
S. 7(1) (2) and (3) Illegal Data Interference			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
1. Intentionally and unlawfully			
a)- Damages or deteriorates - computer data OR b)-Deletes computer Data OR c)-Alters computer Data OR d)-Renders computer data meaningless,	Computer data" has the meaning ascribed to it under S.3	<ul style="list-style-type: none"> <li>- Login or Logout details</li> <li>- Data which has been altered or destroyed or damaged or obstructed or interfered</li> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of Seizure</li> <li>- Cyber</li> </ul>	<ul style="list-style-type: none"> <li>- System administrator</li> <li>- Person who conducted the search</li> <li>- independent witness (if any)</li> <li>- Cyber forensic Expert</li> </ul>

useless or ineffective OR e)-Obstruct, interrupts or interferes with the lawful use of computer data OR f)-Denies access to a computer data to any person authorized to access it		forensic analysis Report - Security measures involved	
2. A person a) Communicates OR discloses OR transmit - Any computer data OR program OR access code OR command - To unauthorized persons		- Login or logout details (data access) - Transmission of data (to and from) - List of authorized persons to the data in question - Modes of transmission - Device or software used	- System Administrator/ owner of the data - Cyber forensic Expert - Person conducting the search - Independent witness (if any) - Authorized persons

		<ul style="list-style-type: none"> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> </ul>	
3	<ul style="list-style-type: none"> <li>- Any person</li> <li>- Intentionally and Unlawful</li> <li>-Destroy OR alters</li> <li>-computer data</li> <li>-Where such data is required to be maintained by law OR is evidence to any proceeding s by</li> <li>a) Mutilatin-g OR Removin-g OR modifyin g the data OR program or any other</li> </ul>	<ul style="list-style-type: none"> <li>- Login or Logout details (data access)</li> <li>- Transmission of data (to and from)</li> <li>- List of authorized persons to the data in question</li> <li>- Modes of transmission</li> <li>- Device or software used</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> </ul>	<ul style="list-style-type: none"> <li>- System Administrator/ owner of the data</li> <li>- Cyber forensic Expert</li> <li>- A person conducting a search</li> <li>- Independent witness</li> <li>- Authorized persons</li> </ul>

<p>form        - information        existing        within or        outside        - computer        system</p> <p>OR</p> <p>b) - Activating        OR        Installing        OR        Downloading</p> <p>- a program        that is        designated        to mutilate        or remove        or modify</p> <p>- data or        program or        any other        form of        information</p> <p>- existing        within or        outside a</p> <p>- computer        system</p> <p>OR</p> <p>c)-Creating        OR Altering        OR        Destroying        -a password</p>			
--	--	--	--

OR Personal identification number OR code or method used to -access a computer data			
--	--	--	--

## MODEL CHARGE STATEMENT OF OFFENCE

**ILLEGAL DATA INTERFERENCE;** Contrary to Section 7(1)(a) of the Cybercrimes Act No. 14 of 2015 read together with paragraph 36 of the First Schedule to, and Sections 57(1) and 60 (2) of the Economic and Organized Crime Control Act [[Cap 200 R.E. 2022]].

### PARTICULARS OF OFFENCE

**CLEY KAT**, on 7<sup>th</sup> December, 2023 at Hazina Street within Arusha District in the Region of Arusha, did intentionally and unlawfully damage computer data namely .....(insert name the kind of computer data e.g. representation of facts or concept or information).

OFFENCE			
[S. 8(1) and(2) Data Espionage			
ELEMENTS	CLARIFICATIONS	POSSIBLE	WITNESS

		<b>EVIDENCE</b>	
<ul style="list-style-type: none"> <li>- Obtaining a computer data protected against unauthorized access</li>   <li>- Without permission</li> </ul>		<ul style="list-style-type: none"> <li>- Login or logout details (data access)</li> <li>- Transmission of data (sender, data and receiver)</li> <li>- Authorized personnel to the data in question</li> <li>- Modes of transmission</li> <li>- Device or software used</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- System Administrator</li> <li>- Cyber forensic Expert</li> <li>- Person who conducted search</li> <li>- Independent witness (if any)</li> </ul>

## **MODEL CHARGE**

### **STATEMENT OF OFFENCE**

**DATA ESPIONAGE;** Contrary to Section 8(1) of the Cybercrimes Act No. 14 of 2015 read together with Paragraph 36 of the First Schedule to, and Section 57(1) and 60 (2) of the Economic and Organized Crime Control Act [[Cap 200 R.E. 2022]].

### **PARTICULARS OF OFFENCE**

**JA,** on 27<sup>th</sup> May, 2018 at Posta area within Ilala District in Dar es Salaam Region, did obtain computer data protected against unauthorized access namely .....(insert the type of computer data e.g. representation of facts or concept or information) without permission.

<b>OFFENCE</b>			
S. 9 Illegal System Interference			
<b>ELEMENTS</b>	<b>CLARIFICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-Intentionally and Unlawful -hinders OR interferes with  a)-the functioning of a computer system  OR	Computer system means a device which includes; a) a computer program, code, software or application  b) Component of computer system such as graphic card,	- Login or logout details (data access)  - Transmission of data (to and from)  - List of authorized persons to the data in	- Cyber forensic Expert  - System administrator  - Person conducting the search  - independent witness (if

b)-The usage OR Operation of a computer system	Memory card, chip or processor c) computer storage component; input and output devices;	question - Modes of transmissio n - Device or software used - Certificate of seizure - Cyber forensic analysis Report - Proof of Chain of custody (oral, documentar y or any other form)	any)
--	--	---	------

### MODEL CHARGE STATEMENT OF OFFENCE

**ILLEGAL SYSTEM INTERFERENCE;** Contrary to Section 9 (a) of the Cybercrimes Act No. 14 of 2015 read together with Paragraph 36 of the First Schedule to, and Section 57(1) and 60 (2) of the Economic and Organized Crime Control Act [[Cap 200 R.E. 2022]].

### PARTICULARS OF OFFENCE

**PK,** on 7<sup>th</sup> December, 2023 at Majengo area within Moshi District in Kilimanjaro Region, did intentionally and unlawfully hinder interfere with the functions of a

computer system to wit .....(insert kind of computer system eg application or computer program or software and mode of hindrance or interference)

<b>OFFENCE</b>			
S. 10(1) (a) (b) and (2) Illegal Device			
<b>ELEMENTS</b>	<b>CLARIFICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
<ul style="list-style-type: none"> <li>-Unlawfully deal with OR posses</li> <li>a)</li> <li>-A device including a computer program</li> <li>-designed OR adopted for the purpose of committing an offence</li> <li>OR</li> <li>b)</li> <li>- A computer password OR access code OR similar data</li> <li>- the whole or any part of a computer system</li> </ul>	<p>A device includes</p> <ul style="list-style-type: none"> <li>a) a computer program, code, software or application</li> <li>b) Component of computer system such as graphic card, Memory card, chip or processor</li> <li>c) computer storage component; input and output devices.</li> </ul>	<ul style="list-style-type: none"> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- Person who conducted search</li> <li>- Independent witness if any</li> </ul>

<ul style="list-style-type: none"> <li>- capable of being accessed</li> <li>- with the intent</li> <li>- be used by any person</li> <li>- for the purpose of committing an offence</li> </ul>			
---	--	--	--

## MODEL CHARGE STATEMENT OF OFFENCE

**ILLEGAL DEVICE** ; Contrary to Section 10(1) (a) of the Cybercrimes Act No. 14 of 2015 read together with Paragraph 36 of the First Schedule to, and Sections 57(1) and 60(2) of the Economic and Organized Crime Control Act [[Cap 200 R.E. 2022]].

### PARTICULARS OF OFFENCE

**CD**, on 22<sup>nd</sup> July, 2019 at Kilakala area within Morogoro District in Morogoro Region, did unlawfully deal with/possess a device to wit ..... (Name the type of device eg computer programme or software or application) designed/ adapted for the purpose of committing an offence namely ..... (Insert name the offence committed)

<b>OFFENCE</b>			
S. 11(1) and (2) Computer Related Forgery			
<b>ELEMENTS</b>	<b>CLARIFICATION</b>	<b>POSSIBLE</b>	<b>WITNESS</b>

		<b>EVIDENCE</b>	
<ul style="list-style-type: none"> <li>-Intenationally and Unlawful</li> <li>-inputs OR alters OR delay transmission OR delete</li> <li>-computer data</li> <li>-Resulting in unauthentic data</li> <li>-with the intent that it be acted upon as if it were authentic</li> </ul>		<ul style="list-style-type: none"> <li>- Login or logout details (data access)</li> <li>- Computer data –</li> <li>- Modes of transmission</li> <li>- Device used</li> <li>- Software used</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- System Administrator</li> <li>- Cyber forensic Expert</li> <li>- Person who conducted the search</li> <li>- Independent witness (if any)</li> </ul>

## **MODEL CHARGE**

### **STATEMENT OF THE OFFENCE**

**COMPUTER RELATED FORGERY;** Contrary to Section 11(1) of the Cybercrimes Act No. 14 of 2015 read together with Paragraph 36 of the First Schedule to, and Sections 57(1) and 60 (2) of the Economic and Organized Crime Control Act [[Cap 200 R.E. 2022]].

## **PARTICULARS OF THE OFFENCE**

**IM** on various dates between 06<sup>th</sup> day of April, 2019 and 16<sup>th</sup> day of February, 2019 at Nyamapinda area, within Ludewa District in Njombe Region, did intentionally and unlawfully input/alter/delay transmission/ delete computer data to wit ..... (Insert type of computer data e.g. representation of facts or concept or information) with intent that it be acted upon as if it were authentic.

<b>OFFENCE</b>			
S. 12(1) and (2) Computer Related Fraud			
<b>ELEMENTS</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
a)-fraudulent OR dishonest intent -cause a loss of property to another person -Input OR alteration OR deletion OR delaying transmission OR suppression of computer data b)-fraudulent OR with		<ul style="list-style-type: none"><li>- Login or logout details (data access)</li><li>- Computer data</li><li>- Modes of transmission</li><li>- Device used</li><li>- Software used</li><li>- Certificate of seizure</li><li>- Cyber forensic analysis Report</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li></ul>	<ul style="list-style-type: none"><li>- System Administrator</li><li>- Cyber forensic Expert</li><li>- Person who conducted the search</li><li>- Independent witness (if any)</li></ul>

dishonest intent -cause a loss of property to another person -Interference with functioning of a computer system			
--	--	--	--

## **MODEL CHARGE**

### **STATEMENT OF THE OFFENCE**

**COMPUTER RELATED FRAUD:** Contrary to Section 12(1) (a) of the Cyber Crimes Act, 2015 read together with Paragraph 36 of the First Schedule to, and Sections 57(1) and 60 (2) of the Economic and Organized Crime Control Act [ 200 R.E. 2022].

### **PARTICULARS OF THE OFFENCE**

**CHAGU** on various dates between 06<sup>th</sup> April, 2019 and 16<sup>th</sup> February, 2020 at Sima area, within Bariadi District in Simiyu Region, fraudulently/ with dishonest intent, did cause the loss of TZS. 2,103,000/= the property of MAIMUNA MZURI, by altering the password of M-PESA account bearing the name of MAIMUNA MZURI.

<b>OFFENCE</b>
S. 13(1), (2) and (3)Child pornography

ELEMENTS	CLARIFICATIONS	POSSIBLE EVIDENCE	WITNESS
a)-Publish -child pornography -through a computer system  OR b)-make available or facilitate -child pornograp- hy -through a computer system	Publish means as defined under Section 3 of the Cyber Crimes Act.  -Child means as defined under S.3.  -“child pornography” means as defined under S.3  -Computer system means as defined under S.3	- Publication (content published) - Mode used to publish - Device or software used for publication - Certificate of seizure - Cyber forensic analysis Report - Proof of Chain of custody (oral, documentary or any other form)	- Cyber forensic Expert - Person who conducted the search - Independent witness (if any)

## MODEL CHARGE STATEMENT OF OFFENCE

**CHILD PORNOGRAPHY:** Contrary to Section 13(1) (a), (2) and (3) of the of Cyber Crimes Act, No. 14 of 2015.

### PARTICULARS OF OFFENCE

**PC**, on 14<sup>th</sup> day of February, 2023, Illembula area within Wanging'ombe District in the Region of Njombe, did publish a child pornography by(insert mode of publication) through a computer system, namely

.....(insert the computer system e.g. WhatsApp, Instagram) .

<b>OFFENCE</b>			
S. 14(1) and (2) Pornography			
ELEMENTS	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
a)-Publish OR cause to be published -through a computer system OR any other information and Communication technology -pornographic material	-pornography as defined under S.3  -computer system as defined under S.3	<ul style="list-style-type: none"> <li>- Mode used to publish</li> <li>- Device used</li> <li>- software used</li> <li>- publication</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- Person who conducted the search</li> <li>- Independent witness (if any)</li> </ul>
b)-Publish OR cause to be published -through a computer system OR any other information and communication technology -pornographic			

material which is lascivious OR obscene			
---	--	--	--

## **MODEL CHARGE** **STATEMENT OF OFFENCE**

**PUBLICATION OF PORNOGRAPHY:** Contrary to Section 14(a) and 2(a) of the Cyber Crimes Act, No. 4 of 2015.

### **PARTICULAR OF OFFENCE**

**MAMBA SHIDA**, on 31<sup>st</sup> day of December, 2022 in Kwamkolemba area within Ilala District in the Region of Dar es Salaam, did publish/cause to be published pornographic material through a computer system or any other information and communication technology to wit .....(insert the computer system or other information and communication technology e.g. Instagram or WhatsApp).

<b>OFFENCE</b>			
S. 15(1) and (2) Personation			
<b>ELEMENTS</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-use of a Computer system -false representation		<ul style="list-style-type: none"> <li>- Computer system used</li> <li>- Mode of publication</li> <li>- A person impersonated</li> </ul>	<ul style="list-style-type: none"> <li>- A person to whom the false representation was made</li> </ul>

-to another person	<ul style="list-style-type: none"> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Publication(content of impersonation)</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- A person who conducted the search</li> <li>- Independent witness (if any)</li> </ul>
--------------------	--	--

## MODEL CHARGE STATEMENT OF OFFENCE

**PERSONATION:** Contrary to Section 15(1) and (2) of the Cybercrimes Act No. 14 of 2015.

### PARTICULARS OF OFFENCE

**HASARA KUJUANA**, on the 26<sup>th</sup> July, 2022 at unknown place within the United Republic of Tanzania by using a computer system to wit (name computer system eg. Instagram, WhatsApp, mobile phone) with intent to defraud one LIWALO NALIWE falsely represented himself as Hon. MATATA MAJUNGU, a Minister for Home Affairs.

<b>OFFENCE</b>			
S. 16 Publication of False Information			
<b>ELEMENTS</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>

<ul style="list-style-type: none"> <li>-Publication</li> <li>-Information OR Data presented in a picture OR text OR symbol OR any other form</li> <li>-In a computer system</li> <li>-knowing that such information OR data is false OR deceptive OR misleading OR inaccurate</li> <li>-with intent to defame OR threaten OR abuse OR insults OR otherwise deceive or Mislead the public OR concealing commission of an offence</li> </ul>		<ul style="list-style-type: none"> <li>- Device used</li> <li>- software used</li> <li>- Mode of publication</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Publication( Proof of Chain of custody oral, document - ary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- Person who conduct the search</li> <li>- Independent witness (if any)</li> <li>- Receiver of the falsely published information/a person to disprove the false information</li> </ul>
--	--	---	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**PUBLICATION OF FALSE INFORMATION:** Contrary to Section 16 of the Cybercrimes Act No. 14 of 2015.

## **PARTICULARS OF OFFENCE**

**MJUZI MJANJA**, on 15<sup>th</sup> November 2022 within the United Republic of Tanzania, did publish a false information to wit "**HATIMAYE SERIKALI YARUHUSU BANGI**" in a computer system namely .....(insert the computer system eg Facebook or Instagram or WhatsApp) with intent to mislead the public while knowing that such information to be false.

<b>OFFENCE</b>			
S. 17(1) and (2) Production/ Offer/ Distribute of Racist or Xenophobic material			
<b>ELEMENTS</b>	<b>CLARIFICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-through a computer system a)-Produce racist OR xenophobic materials -for the purposes of distribution OR b)-offer OR	Racist and Xenophobic material" means as defined in S.3	<ul style="list-style-type: none"><li>- Device used</li><li>- software used</li><li>- Mode of publication</li><li>- Logs details</li><li>- Cyber forensic analysis Report</li><li>- Certificate of seizure</li><li>- Publication(content of racist or xenophobic materials)</li></ul>	<ul style="list-style-type: none"><li>- Cyber forensic Expert</li><li>- Person who conducted search</li><li>- Independent witness (if any)</li></ul>

make available -racist or xenoph - obic materials OR c)- distributes OR transmit racist -xenophob ic materials -name of the complain- ant		- Proof of Chain of custody (oral, documentary or any other form) - Evidence to establish how the complainant was affected by the Xenophobic Material	
---	--	--	--

## MODEL CHARGE STATEMENT OF OFFENCE

**DISTRIBUTION OF RACIST MATERIAL:** Contrary to Section 17(1)(c) and (2) of the Cybercrimes Act No. 14 of 2015.

### PARTICULARS OF OFFENCE

**PY**, on 26<sup>th</sup> September, 2018 at Ngudu area within Kwimba District in Mwanza Region, did distribute through a computer system to wit .....  
(Name of a computer system e.g. Instagram, Facebook or YouTube) a racist material namely

..... (e.g. A picture of Gorrilla to refer to (insert the name of the complainant)

<b>OFFENCES</b>				
S. 18(1) and (2) Racist or xenophobic insult				
<b>ELEMENT</b>	<b>CLARIFICATIONS</b>	<b>EVIDENCE TO PROVE</b>	<b>WITNESS</b>	
i. Insult another person  ii. Through a computer system  iii. On the basis of race OR colour OR descent OR nationality OR ethnic origin OR religion		<ul style="list-style-type: none"> <li>- Device used –</li> <li>- Software used</li> <li>- Mode of publication</li> <li>- Login or logout details</li> <li>- Cyber forensic analysis Report</li> <li>- Certificate of seizure</li> <li>- Publication(content of racist or xenophobic motivated to insult)</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> <li>- Evidence to establish how the victim/Complainant was affected by the Xenophobic insult.</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- A person who conducted a search</li> <li>- Independent witness (if any)</li> </ul>	

## **MODEL CHARGE** **STATEMENT OF OFFENCE**

**PUBLICATION OF RACIST INSULTS:** Contrary to Section 18(1)(c) and (2) of the Cybercrimes Act No. 14 of 2015.

### **PARTICULARS OF OFFENCE**

**PY**, on 26<sup>th</sup> September, 2018 Ngudu area within Kwimba District in Mwanza Region, did publish a racist insults to wit..... (Insert the racist insult words) through his Facebook account (insert name of the Facebook account) ..... (.....to refer to (insert name of the victim)

<b>OFFENCES</b>			
S. 19(1),(2) and (3) Publication of Genocide / Crimes against humanity material.			
<b>ELEMENTS</b>	<b>CLARIFICATION</b>	<b>EVIDENCE POSSIBLE</b>	<b>WITNESS</b>
- unlawfully publish OR cause to be published -through a computer system -material which incites OR denies OR minimizes OR justifies -acts constituting	Genocide has the meaning ascribed to it under the Convention on the Prevention and punishment of the Crime of Genocide, 1948.	A report of the Cyber forensic Expert. Print-out of the publication Computer device used.	Cyber forensic Expert, Officer conducting search, Independent witness if any Investigator System administrator

genocide or crime against humanity			
------------------------------------	--	--	--

## **MODEL CHARGE**

### **STATEMENT OF OFFENCE**

**PUBLICATION OF GENOCIDE MATERIAL:** Contrary to Section 19(1)( and (2) of the Cybercrimes Act No. 14 of 2015 read together with paragraph 36 of the First Schedule to, and Sections 57(1) and 60(2) of the Economic and Organized Crime Control Act [Cap 200 R.E. 2022].

### **PARTICULARS OF OFFENCE**

ZY, on 30<sup>th</sup> June, 2023 in at Shirati area within Rarya District in Mara Region, did unlawfully publish /cause to be published a genocide material to wit .....( insert the genocide material published) through his a YouTube/ Instagram/ Facebook, Tiktok account ..... which incites/denies/minimises/justifies acts constituting genocide.

<b>OFFENCES</b>			
S. 20(1), (2) and (3) initiate transmission/ relay/ re transmit/ falsify header Unsolicited Messages			
<b>ELEMENTS</b>	<b>CLAFIRICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-With intent to commit an	Unsolicited messages" means as defined under	- Report from the service provider Sim	- Service provider - A person

offence under this Act a.-Initiate the transmission of unsolicited messages -relay or retransmit unsolicited messages -falsify header information in unsolicited message	S. 20 (3) “service provider” means as defined under S 3	card registration details or any other means used - Device used - software used - Certificate of seizure - Cyber forensic analysis report - Proof of Chain of custody (oral, documentary or any other form)	who conducted the search - Independent witness (if any) - Victims of crime - Cyber forensic expert
---	--	--	---

## MODEL CHARGE STATEMENT OF OFFENCE

**INITIATE UNSOLICITED MESSAGE:** Contrary to Section 20(1)(a) of the Cybercrimes Act No. 14 of 2015.

### **PARTICULARS OF OFFENCE**

**IST**, on 8<sup>th</sup> August, 2023 at Kihesa area within Iringa District in Iringa Region, with an intent to defraud (insert name of complainant)..... By using a computer system), initiated the transmission of unsolicited message which reads ..... (Mention the unsolicited message).

<b>OFFENCES</b>			
S. 21(1) and (2) Disclosure of details of Investigation			
<b>ELEMENTS</b>	<b>CLARIFICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-Knowingly and Unlawfully disclose details of criminal investigation -which Requires confidentiality.		<ul style="list-style-type: none"> <li>- Presence of a criminal Case file under investigation</li> <li>- Mode of disclosure of investigation</li> <li>- To whom the disclosure was done</li> <li>- Device of software used (if any)</li> <li>- Certificate of seizure</li> <li>- Information disclosed</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Owner of the data base (service provider)</li> <li>- Person who conducted search</li> <li>- Independent witness (if any)</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**  
**DISCLOSURE OF INVESTIGATION DETAILS;**  
 Contrary to Section 21(1)(a) and (2) of the Cybercrimes  
 Act No. 14 of 2015.

## **PARTICULARS OF OFFENCE**

**PAREJO**, on 9<sup>th</sup> January, 2021 at Mbekenyela area within Ruangwa District in the Region of Lindi, knowingly and unlawfully disclosed details of a criminal investigation to wit .....  
 (things/information disclosed) which requires confidentiality.

<b>OFFENCES</b>			
S. 22(1) Obstruction of investigation			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>ELEMENTS TO PROVE</b>	<b>WITNESS</b>
1)- Intentionally and unlawfully -destroys OR delete OR alter OR conceal OR modify OR Renders computer data meaningless or ineffective or useless. -with intent to obstruct or delay investigation		<ul style="list-style-type: none"> <li>- Presence of a criminal Case file for the existing investigation</li> <li>- Mode of obstruction of investigation</li> <li>- Device or software used (if any)</li> <li>- Cyber forensic analysis Report</li> <li>- Certificate of seizure</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>-system administrator</li> <li>-owner of the system</li> <li>-person who conducted the search</li> <li>-Independent witness (if any)</li> <li>-cyber forensic expert</li> </ul>
2)-Intentionally and unlawfully -Prevent the			

Execution OR Fail to comply with an order issued under this Act.			
--	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**OBSTRUCTION OF INVESTIGATION:** Contrary to Section 22(1) of the Cybercrimes Act No. 14 of 2015.

**PARTICULARS OF OFFENCE**

**GL**, on 18<sup>th</sup> November, 2020 at Kiomboi area within Iramba District in the Region of Singida, intentionally and unlawfully, did alter computer data to wit NMB SIM BANKING SOFTWARE rendering it meaningless with intent to obstruct investigation.

<b>OFFENCE</b>			
S. 23(1) and (2) Cyber Bullying			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>

<ul style="list-style-type: none"> <li>-Initiate OR send electronic communication</li> <li>-Using a computer system</li> <li>-to another person</li> <li>-With intent to coerce OR intimidate OR harass OR cause emotional distress</li> </ul>		<ul style="list-style-type: none"> <li>- Publication</li> <li>- Device used</li> <li>- software used</li> <li>- login or logout details</li> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> <li>- Mode of publication</li> <li>- Know your customer</li> <li>- Instagram, Facebook, or any other account name</li> </ul>	<ul style="list-style-type: none"> <li>- Person conducting the search</li> <li>- Independent witness (if any)</li> <li>- Cyber forensic Expert</li> <li>- Victim of a crime</li> <li>- Service provider</li> <li>- investigator</li> </ul>
--	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**CYBER BULLYING:** Contrary to Section 23(1) and (2) of the Cybercrimes Act No. 14 of 2015.

## **PARTICULARS OF OFFENCE**

**MK**, on 1<sup>st</sup> December, 2023 at Mbezi beach area within Kinondoni District in the City and Region of Dar es Salaam, did send electronic communication namely video recording of NEI KOI using a computer system to wit ..... (Insert the computer system e.g. WhatsApp or Instagram) to ..... (Insert the person to whom the electronic communication was sent to) with intent to coerce.

<b>OFFENCES</b>			
S. 24(1) and (2) Violation of Intellectual property rights			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-Use a computer system -With intent to violate intellectual property rights protected under any written law		<ul style="list-style-type: none"><li>- Publication</li><li>- Device or software used</li><li>- Certificate of seizure</li><li>- Cyber forensic analysis Report</li><li>- Mode of publication</li><li>- Registered intellectual property right</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li><li>- Whether the infringement</li></ul>	<ul style="list-style-type: none"><li>- Victim of a crime</li><li>- Cyber forensic Expert</li><li>- A person who conducted search</li><li>- Independent witness (if any)</li><li>- An officer from COSOTA</li></ul>

		<p>is on commercial or non- commercial basis</p> <ul style="list-style-type: none"> <li>- Intellectual property right</li> </ul>	
--	--	--	--

## MODEL CHARGE STATEMENT OF OFFENCE

**VIOLATION OF INTELLECTUAL PROPERTY RIGHTS:** Contrary to Section 24(1) and 2(b) of the Cybercrimes Act No. 14 of 2015.

### PARTICULARS OF OFFENCE

DP, on 3<sup>rd</sup> March, 2021, at Masaki area within Kinondoni District in the Region of Dar es Salaam, did upload music namely .....(insert the music name) by using a computer system namely .....(insert the computer system eg BOOMPLAY or YOTUBE) to .....(the property of .....(insert the name of the owner of the video) with intent to violate intellectual property right.

OFFENCES			
S. 27 Conspiracy to commit an offence			
ELEMENT	CLARIFICATIONS	EVIDENCE TO PROOF	WITNESS
Agreement -with another person		<ul style="list-style-type: none"> <li>- KYC</li> <li>- Intended cybercrime</li> </ul>	<b>Investigator</b> <b>Cybercrime</b> <b>forensic</b>

-to commit an offence		<ul style="list-style-type: none"> <li>- to be committed</li> <li>- Modes of communication used for conspiracy</li> <li>- The actual commission of that other cybercrime</li> </ul>	<b>expert complainant</b>
-----------------------	--	---	---------------------------

## **MODEL CHARGE** **STATEMENT OF OFFENCE**

**CONSPIRACY:** Contrary to Section 27 of the Cybercrimes Act No. 14 of 2015.

### **PARTICULARS OF OFFENCE**

**SJ** and **EW** on diverse dates between 29<sup>th</sup> September, 2023 and 5<sup>th</sup> December, 2023 within Korogwe District in Tanga Region and Ilala District in the Region of Dar es Salaam, jointly and together, did conspire to commit an offence of cyber bullying.

### **B. THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT [CAP 306 RE 2022]**

<b>OFFENCE</b>			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-Installs OR	Network facility is	<ul style="list-style-type: none"> <li>- Device or</li> </ul>	<ul style="list-style-type: none"> <li>- Person who</li> </ul>

<p>operates OR constructs OR maintains OR owns OR makes available - network facilities -without obtaining any relevant individual licence,</p>	<p>as defined under S. 3</p>	<p>software used</p> <ul style="list-style-type: none"> <li>- Certificate of seizure</li> <li>- Cyber forensic analysis Report</li> <li>- Actual loss report from TCRA</li> <li>- Report from TCRA proving no license has been issued to the accused (if any)</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> <li><b>- Search Warrant if any</b></li> </ul>	<p>conducted the search</p> <ul style="list-style-type: none"> <li>- Independent witness (if any)</li> <li>- Cyber forensic Expert</li> <li>- TCRA officer</li> <li>- Cyber forensic Expert</li> <li>-</li> <li>- Independent witness (if any)</li> </ul>
--	------------------------------	---	---

### OFFENCE

S. 116(2) provision of network services without obtaining any relevant individual licence

ELEMENTS	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
<p>-Provide network services without</p>		<ul style="list-style-type: none"> <li>- Device or software used</li> <li>- Certificate of</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- Person who</li> </ul>

obtaining any relevant individual licence,		<p>seizure</p> <ul style="list-style-type: none"> <li>- independent witness (if any)</li> <li>- Cyber forensic analysis Report</li> <li>- Actual loss report from TCRA</li> <li>- Report from TCRA proving no license has been issued to the accused</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<p>conducted the search</p> <ul style="list-style-type: none"> <li>- independent witness (if any)</li> <li>- TCRA officer</li> <li>- Licence</li> </ul>
--	--	--	---

### **OFFENCES**

S. 116(3)(a) provision of application services without obtained any relevant individual licence

<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
a)-provide application services -without		<ul style="list-style-type: none"> <li>- Device or software used</li> <li>- Certificate of</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber forensic Expert</li> <li>- Person who</li> </ul>

<p>obtaining any relevant individual licence</p> <p>OR</p> <p>b)-provision content services without obtaining any relevant individual licence</p> <p>c)-Imports OR distributes</p> <ul style="list-style-type: none"> <li>-electronic Communication equipment or apparatus</li> <li>-without a licence</li> <li>-establishes OR installs OR maintains and operates</li> <li>-an electronic</li> </ul>		<p>seizure</p> <ul style="list-style-type: none"> <li>- Cyber forensic analysis Report</li> <li>- Actual loss report from TCRA</li> <li>- Report from TCRA proving no license has been issued to the accused</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<p>conducted the search</p> <ul style="list-style-type: none"> <li>- independent witness (if any)</li> <li>- TCRA officer</li> <li>- Licence</li> </ul>
---	--	--	---

communication system -without a licence			
OR -imports -non type approved electronic communication equipment or apparatus into the United Republic -without a licence			

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**INSTALLATION/OPERATION/MANTAINING/CONSTRUCTION OF NETWORK FACILITIES WITHOUT OBTAINING RELEVANT INDIVIDUAL LICENSE**  
Contrary to Section 116(1) of the Electronic and Postal Communications [[Cap 306 R.E. 2022]]

**PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on diverse dates between 13<sup>th</sup> August, 2022 and 22<sup>nd</sup> October, 2022 at Mbezi beach

area within Kinondoni District in Dar es Salaam Region, did .....(insert relevant offence)in, Electronic Communication equipment to wit; SIM BOX/VOIP GATEWAY make DINSTAR with serial number DBOO-0030-1901-3000 in the United Republic of Tanzania without obtaining relevant Individual license issued by Tanzania Communications Regulatory Authority.

**STATEMENT OF OFFENCE**

**PROVISION OF NETWORK SERVICES WITHOUT OBTAINING RELEVANT INDIVIDUAL LICENSE,**  
Contrary to Section 116(2)(c) of the Electronic and Postal Communications [[Cap 306 R.E. 2022]]

**PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on diverse dates between 13<sup>th</sup> July, 2021 and 22<sup>nd</sup> November, 2022 at Mbezi beach within Kinondoni District in Dar es Salaam Region, did provide network service .....(insert name of the Service) in the United Republic of Tanzania without obtaining relevant Individual license issued by Tanzania Communications Regulatory Authority.

OR

**STATEMENT OF OFFENCE**

**PROVISION OF APPLICATION SERVICE WITHOUT OBTAINING RELEVANT INDIVIDUAL LICENSE,**

Contrary to Section 116(3)(a) of the Electronic and Postal Communications [Cap 306 R.E. 2022]

### **PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on diverse dates between 13<sup>th</sup> July, 2021 and 22<sup>nd</sup> November, 2022 at Mbezi beach within Kinondoni District in Dar es Salaam Region, did provide Application Service.....(insert the name of Application service provided) in the United Republic of Tanzania without obtaining relevant Individual license issued by Tanzania Communications Regulatory Authority.

### **STATEMENT OF OFFENCE**

**PROVISION OF CONTENT SERVICE WITHOUT OBTAINING RELEVANT INDIVIDUAL LICENSE,**  
Contrary to Section 116(3) (b) of the Electronic and Postal Communications [Cap 306 R.E. 2022]

### **PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on diverse dates between 13<sup>th</sup> July, 2021 and 22<sup>nd</sup> November, 2022 at Mbezi beach within Kinondoni District in Dar es Salaam Region, did provide content service.....(insert the Content service provided) in the United Republic of Tanzania without obtaining relevant Individual license issued by Tanzania Communications Regulatory Authority.

## **STATEMENT OF OFFENCE**

**IMPORTATION/DISTRIBUTION/ESTABLISHMENT/INSTALLATION/MANTAINING/OPERATING OF AN ELECTRONIC COMMUNICATION SYSTEM OR EQUIPMENT WITHOUT LICENSE; Contrary to Section 116(3)(c) of the Electronic and Postal Communications [Cap 306 R.E. 2022]**

## **PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on diverse dates between 13<sup>th</sup> July, 2021 and 22<sup>nd</sup> November, 2022 at Mbezi beach within Kinondoni District in Dar es Salaam Region, did .....(insert the relevant offence committed) in the United Republic of Tanzania without obtaining license issued by Tanzania Communications Regulatory Authority.

<b>OFFENCES</b>			
S. 117(1) use of radio frequency spectrum without obtaining individual assignment			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
1)-uses -radio frequency spectrum -without obtaining any relevant individual assignment,	-Radio communication has a meaning as ascribed under S.3 -Individual assignment has a meaning as ascribed under	- Device or software used - Report of loss incurred from TCRA - Proof of absence of	- TCRA licensing officer - person conducting search - independent witness (if any)

	S.3	assignment - Licence - Certificate of seizure	
<b>OFFENCE</b>			
S. 117(3) use of number/ electronic address without obtaining individual/class assignment			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
3)-use of one or more numbers or electronic addresses -without having first obtained any relevant individual assignment, or any relevant class assignment,		<ul style="list-style-type: none"> <li>- Device or software used</li> <li>- Report of loss from TCRA</li> <li>- Proof of absence of assignment</li> <li>- Licence</li> <li>- Certificate of seizure</li> </ul>	<ul style="list-style-type: none"> <li>- TCRA licensing officer</li> <li>- person conducting search</li> <li>- independent witness (if any)</li> <li>- Spectrum Engineers</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**USE OF RADIO FREQUENCY SPECTRUM WITHOUT OBTAINING RELEVANT INDIVIDUAL ASSIGNMENT;**  
 Contrary to Section 117(1) of the Electronic and Postal Communications [Cap 306 R.E. 2022]

## **PARTICULARS OF OFFENCE**

**HAKUNA MATATA** owner of **MATATA FM**, on diverse dates between 20<sup>th</sup> May, 2018 and 30<sup>th</sup> January, 2020 at Kariakoo area within Ilala District in Dar es Salaam Region, did use radio frequency spectrum .....(insert radio frequency eg. Megahertz MHz) without obtaining relevant individual assignment from Tanzania Communications Regulatory Authority.

<b>OFFENCES</b>			
S. 118(a) Transmission of obscene communication			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
1) a)-any means of any network facilities OR network services OR applications services OR content services -knowingly -makes OR creates, OR solicits OR initiates -the Transmission of -any comment OR request OR suggestion OR other Communication		<ul style="list-style-type: none"> <li>- Device or software used</li> <li>- Mode of Transmission</li> <li>- Cyber Forensic report</li> <li>- Seizure certificate</li> <li>- Logs details</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Independent witness (if any)</li> <li>- TCRA officer</li> <li>- Owner of the system/Service Provider</li> </ul>

<ul style="list-style-type: none"> <li>-which is obscene, indecent, false, menacing or offensive in character</li> <li>-with intent to annoy, abuse, threaten or harass another person</li> </ul> <p>b)-Initiates a communication</p> <ul style="list-style-type: none"> <li>-using any applications services,</li> <li>-whether continuously, repeatedly or otherwise,</li> <li>-during which Communication may or may not ensue,</li> <li>-with or without disclosing his identity</li> <li>-with intent to annoy, abuse, threatens or harass any person</li> <li>-at any number or electronic address;</li> </ul>			
--	--	--	--

<p>OR</p> <p>c) -By means of any network services or applications service        -provides any obscene communication        -to any person;</p> <p>OR</p> <p>d)-Permits        -any network services OR application services        -under the person's control        -to be used for an activity described in Section 117(3)</p>			
--	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**TRANSMISSION OF OBSCENE COMMUNICATION;**  
 Contrary to Section 118(a) of the Electronic and Postal Communications [Cap 306 R.E. 2022]

## **PARTICULARS OF OFFENCE**

**PRADO PAJERO**, on 30<sup>th</sup> October, 2018 at Mbagala area within Temeke District in Dar es Salaam Region, by use of application namely .....(insert name of Application service used e.g. Facebook, Tiktok ) knowingly made a transmission of a comment to wit .....(insert the comment) which is offensive in nature with intent to annoy .....(insert the person intended).

<b>OFFENCE</b>			
S. 119 Failure to obtain radio frequency spectrum licence			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-use -radio frequency spectrum - without having first obtained any relevant class license		<ul style="list-style-type: none"><li>- Device used</li><li>- Software used</li><li>- TCRA licensing officer</li><li>- Certificate of seizure</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li><li>- Licence</li></ul>	<ul style="list-style-type: none"><li>-TCRA officer</li><li>- person conducting the search</li><li>- Independent witness (if any)</li></ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**USE OF RADIO FREQUENCY SPECTRUM WITHOUT LICENCE; Contrary to Section 119 of the Electronic and Postal Communications [Cap 306 R.E. 2022]**

**PARTICULARS OF OFFENCE**

**HAKUNA MATATA** owner of **MATATA FM**, on diverse dates between 20<sup>th</sup> May, 2018 and 30<sup>th</sup> January, 2020 at Kariakoo area within Ilala District in Dar es Salaam Region, did use radio frequency spectrum to wit 88.20 FM without obtaining a licence from Tanzania Communications Regulatory Authority.

<b>OFFENCE</b>			
S. 120 Interception of communications			
<b>ELEMENT</b>	<b>CLARIFICATIONS</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-without lawful authority under this Act or any other written law  a)-Intercepts OR attempts to intercepts OR procures any other person to intercept OR attempt to intercept any communications; OR		- Device or software used - Owner of the system/Service Provider - Mode of interception - Cyber Forensic report - Seizure certificate - Login or	- Cyber Forensic Expert - System administrator - Person conducting the search - Independent witness if any

<p>b)-Discloses OR attempts to disclose -to any other person -the contents of any communications, OR</p> <p><b>c)</b>-uses OR attempts to use -the contents of any communications -knowingly OR having reason to believe -that the information was obtained through the interception of any communications in contravention of this Section</p>		<ul style="list-style-type: none"> <li>- Logout details</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	
---	--	---	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**INTERCEPTION OF COMMUNICATIONS;** Contrary to Section 120 (a) of the Electronic and Postal Communications Act [[Cap 306 R.E. 2022]] read together with paragraph 37 of the First Schedule to, and

Sections 57(1) and 60 (2) of the Economic and Organized Crime Control Act [Cap 200 R.E. 2022].

### **PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, without lawful authority, did intercept communication of one **EM**.

<b>OFFENCE</b>			
S. 121 discloses intercepted communication by Authorized persons			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
<ul style="list-style-type: none"><li>- A person who is authorized under this Act</li><li>- Intentionally</li><li>- discloses OR attempt to disclose to any other person</li><li>- The content of any communications, intercepted by means authorized by this Act</li><li>a) Knowing OR having reason to believe that the information was obtained through the interception of such</li></ul>		<ul style="list-style-type: none"><li>- Device used</li><li>- Software used</li><li>- TCRA licensing officer</li><li>- Certificate of seizure</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li><li>- Licence</li></ul>	<ul style="list-style-type: none"><li>-TCRA officer</li><li>- person conducting the search</li><li>- Independent witness (if any)</li></ul>

<p>communication s in connection with a criminal investigation OR</p> <p>b) Having obtained OR received the information in connection with a criminal investigation OR</p> <p>c) Improperly obstructs impedes OR interferes with a duly authorized criminal investigation</p>			
---	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**  
**DISCLOSURE OF INTERCEPTED COMMUNICATION**  
**BY AUTHORIZED PERSONS;** Contrary to Section  
121(1) (a) of the Electronic and Postal Communications  
Act [Cap 306 R.E. 2022].

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup>  
May, 2019 at Kisasa area within Dodoma District in the  
Region of Dodoma, being an authorized Employee of  
.....(insert name of Telecommunication comp.)

intentionally disclosed intercepted communication related to criminal Investigation to wit;.....(insert content of intercepted communication) communication of one **EM to PW**.

OFFENCE			
S. 122 Fraudulent use of network facilities, network services, application service and content services			
ELEMENT	CLARIFICATIONS	POSSIBLE EVIDENCE	WITNESS
-Dishonestly -transmit OR allows to be transmitted any -Communication-s OR Obtains a service provided by a licensed network facilities provider OR network service provider OR application services provider OR content service provider -With intent to avoid payment of any rate OR fee applicable		<ul style="list-style-type: none"> <li>- Device or software used</li> <li>- Owner of the system/Service Provider</li> <li>- Mode of interception</li> <li>- Cyber Forensic report</li> <li>- Seizure certificate</li> <li>- Login or Logout details</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Cyber Forensic Expert</li> <li>- System administrator</li> <li>- Person conducting the search</li> <li>- Independent witness if any</li> </ul>

<p>to the provision of that facility OR services</p> <p>b)-Possess OR obtains OR creates a system Designed to fraudulently use of obtain any network facilities OR network service OR applications service OR content service</p>			
---	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**FRAUDULENT USE OF NETWORK FACILITIES/  
 NETWORK SERVICE/CONTENT SERVICE/  
 APPLICATION SERVICE;** Contrary to Section 122 (a)  
 of the Electronic and Postal Communications Act [Cap  
 306 R.E. 2022] read together with paragraph 37 of the  
 First Schedule to, and Sections 57(1) and 60 (2) of the  
 Economic and Organized Crime Control Act [Cap 200  
 R.E. 2022].

## **PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, dishonestly transmitted with intent to avoid payment or fee.....(insert the rate of the fee/amount applicable to the provision of that facility )

<b>OFFENCE</b>			
S. 123 (1) and (2) Interfere Transmission of Electronic Communications			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
Interferes with OR obstruct the transmission or reception of any electronic communications		<ul style="list-style-type: none"><li>- Device used</li><li>- Software used</li><li>- TCRA licensing officer</li><li>- Certificate of seizure</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li><li>- Licence</li></ul>	<ul style="list-style-type: none"><li>-TCRA officer</li><li>- person conducting the search</li><li>- Independent witness (if any)</li></ul>

## **MODEL CHARGE**

### **STATEMENT OF OFFENCE**

**INTERFERENCE OF TRANSMISSION OF ELECTRONIC COMMUNICATIONS;** Contrary to Section 123(1)(2) of the Electronic and Postal Communications Act [Cap 306 R.E. 2022] read together with paragraph 37 of the First Schedule to, and Sections 57(1) and 60 (2) of the Economic and Organized Crime Control Act [Cap 200 R.E. 2022].

### **PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, without probable cause , did interfere with electronic communication.....(insert nature or type of communication interfered) of one **EM**.

<b>OFFENCE</b>			
S. 125 Sale, transfer or disposal of SIM cards without authority of network service licensee			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
-Sales OR distributes -any SIM card -Without the authorization of the appropriate network service		-Where and to whom SIM cards were sold/distributed -Number of SIM cards sold/distributed -Certificate of seizure	-TCRA officer - person conducting the search - Independent witness (if any) -Owner of device/service

licensee	<ul style="list-style-type: none"> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> <li>-Identification of sim card sold/distributed without authorization</li> </ul>	provider - service provider/network service licensee
----------	---	---

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**SALE/TRANSFER/DISPOSAL OF SIM CARD WITHOUT;** Contrary to Section 125 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022].

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, sold SIM CARDS, the property of .....(insert name of network service licensee) without license.

OFFENCE			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
	S. 126 possession of mobile telephone or SIM card suspected to have been stolen		

<ul style="list-style-type: none"> <li>-Found in Possession of any</li> <li>-mobile telephone or SIM card</li> <li>-suspected to have been stolen</li> <li>-Without giving satisfactory account of such possession</li> </ul>	<ul style="list-style-type: none"> <li>- Mobile phone or SIM cards found</li> <li>- Certificate of seizure</li> <li>- Mobile phone or SIM card suspected to have been stolen</li> <li>- Certificate of seizure</li> <li>- Details of the owner of the mobile phone or sim card</li> <li>- Records of sim card registration</li> <li>- When was the mobile phone or sim card lost</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> <li>- Receipts(where he/she bought or obtain the mobile phone/sim card and the</li> </ul>	<ul style="list-style-type: none"> <li>- person conducting the search</li> <li>- Independent witness (if any)</li> <li>- Owner of the phone</li> </ul>
---	--	--

		amount -	
--	--	-------------	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**BEING FOUND IN POSSESSION OF MOBILE TELEPHONE/SIM CARD SUSPECTED TO HAVE BEEN STOLEN;** Contrary to Section 126 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022]

**PARTICULARS OF OFFENCE**

**SK**, on 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, was found in possession of .....(insert the SIM CARD or Phone stolen) suspected to have been stolen or unlawfully acquired.

OFFENCE			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
-Acquire OR Receives -a stolen mobile telephone or SIM card from any other person -Without having reasonable cause to		-Stolen mobile or sim card -Certificate of seizure -Details of the owner of the mobile phone or	- person conducting the search -Independent witness (if any) -Owner of a mobile phone

<p>believe that at a time of such acquisition or receipt that mobile phone or SIM card was the property of the person from whom he acquires or receives OR</p> <p>-That person has been duly authorized by the owner to deal with it or dispose of</p>		<p>sim card</p> <p>-Records of sim card registration</p> <p>-When was the mobile phone or sim card stolen</p> <p>-Receipts (where he/she bought or obtain the mobile phone/sim card and the amount</p> <p>-Proof of Chain of custody (oral, documentary or any other form)</p>	
--	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**RECEIVING MOBILE TELEPHONE/SIM CARD SUSPECTED TO HAVE BEEN STOLEN;** Contrary to Section 127 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022]

## **PARTICULARS OF OFFENCE**

**SK**, on 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, received ..... (Insert the SIM CARD or Phone stolen) suspected to have been stolen or unlawfully acquired.

<b>OFFENCE</b>			
S. 128(1) and (3) Failure to report loss or theft or destruction of a mobile phone or SIM card			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
Fails to report the loss OR theft OR destruction of a mobile telephone or SIM card		<ul style="list-style-type: none"><li>- Details of the owner of mobile phone or SIM card</li><li>- Who currently use the mobile phone or SIM card</li><li>- When was mobile phone or SIM card lost</li><li>- Statement of the investigator that no loss was reported</li><li>- Information from the service provider</li><li>- IMEI analysis</li></ul>	<ul style="list-style-type: none"><li>- person conducting the search</li><li>- Independent witness (if any)</li><li>- Officer from service provider</li></ul>

		from service provider	
--	--	-----------------------	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**FAILURE TO REPORT LOSS/THEFT OF MOBILE TELEPHONE OR SIM CARD;** Contrary to Section 128(1) of the Electronic and Postal Communications Act [Cap 306 R.E. 2022]

**PARTICULARS OF OFFENCE**

**SK**, on 4<sup>th</sup> March, 2017 at Kisasa area within Dodoma District in the Region of Dodoma, failed to report the loss/theft/destruction of.....(insert name of the lost/stolen property) to Law Enforcement officer.

OFFENCE			
S. 129 Tempering with mobile telephones or SIM card			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
Intentionally and unlawfully in any manner Tempers OR modifies OR alters OR reconfigures OR interferes with mobile telephone or		<ul style="list-style-type: none"> <li>- Mobile phone or SIM card tempered</li> <li>- Certificate of seizure</li> <li>- Information from service provider in respect of</li> </ul>	<ul style="list-style-type: none"> <li>- person conducting the search</li> <li>- Independent witness (if any)</li> <li>- Cyber forensic expert.</li> </ul>

sim card or any part thereof AND Reverse engineers OR decompiles OR interferes with mobile telephone or SIM card or any part thereof		SIM card tempered <ul style="list-style-type: none"> <li>- Expert report on tempered mobile phone</li> <li>- Cyber forensic analysis report</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	
--	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**TEMPERING WITH MOBILE TELEPHONE /SIM CARD;** Contrary to Section 129(a) of the Electronic and Postal Communications Act [Cap 306 R.E. 2022]

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, intentionally and unlawfully tempered with.....(insert the name of property tempered and its descriptions)

<b>OFFENCE</b>			
S. 130 Failure to record sale of mobile telephones or SIM card			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
Sells OR in any manner provides any mobile telephone or SIM card to any other person Without recording the particulars of that person as required by Section 102 of this Act		<ul style="list-style-type: none"> <li>- Evidence of sale of mobile telephone or SIM card</li> <li>- Details of the mobile phone or SIM card sold/provided in any manner</li> <li>- Statement of the buyer</li> <li>- Statement of the service provider</li> <li>- Sales Register</li> </ul>	<ul style="list-style-type: none"> <li>- person conducting the search</li> <li>- Independent witness (if any)</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**FAILURE TO RECORD SALE OF MOBILE TELEPHONES;** Contrary to Section 130 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022].

### **PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, did sell mobile telephone to .....(insert name of the buyer) without recording the particulars of that person.

<b>OFFENCE</b>			
S. 131(1) Use of Unregistered SIM card			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
Knowingly uses OR causes to be used an unregistered SIM card		<ul style="list-style-type: none"><li>- Identification of the SIM card in question</li><li>- To whom the said SIM cards were assigned by TCRA</li><li>- Statement from TCRA Officer in respect of assignment of SIM cards</li><li>- Statement</li></ul>	<ul style="list-style-type: none"><li>-TCRA officer</li><li>- person conducting the search</li><li>- Independent witness (if any)</li></ul>

		<p>from the service provider to whom the numbers were assigned</p> <ul style="list-style-type: none"> <li>- Certificate of seizure</li> <li>- Statement of independent witness who witnessed the search</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	
--	--	---	--

## **MODEL CHARGE** **STATEMENT OF OFFENCE**

**USE OF UNREGISTERED SIM CARD;** Contrary to Section 131(1) of the Electronic and Postal Communications Act [Cap 306 R.E. 2022].

### **PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, knowingly and with intent to defraud

used unregistered SIM CARD ..... (insert the type of unregistered SIM CARD with descriptions) .

<b>OFFENCE</b>			
S. 132 Furnishing false information or statement			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
Furnishes information OR makes a statement Knowing that such information or statement is false OR incorrect OR misleading OR not believing it to be true		<ul style="list-style-type: none"> <li>- The false information furnished</li> <li>- Mode in which the false information was communicated</li> <li>- Statement of a victim concerned with the false information</li> <li>- Certificate of seizure</li> <li>- Independent witness (if any)</li> <li>- Proof of Chain of custody (oral, documentary or any other form)</li> </ul>	<ul style="list-style-type: none"> <li>- Victim</li> <li>- person conducting the search</li> <li>- Independent witness (if any)</li> </ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**FURNISHING FALSE INFORMATION;** Contrary to Section 132 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022].

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, did furnish Information/statement .....(insert the Statement/Information furnished) knowingly such information/statement is false

OFFENCE			
S. 133 Obstruction to perform duty			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
Obstructs OR Hinders OR Interferes with an authorized person to execute any direction issued under this Act OR assist with the execution thereof		- Presence of directives - Modes of hindering/obstruction	- Person to whom directives were issued

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**OBSTRUCTION TO PERFORM DUTY;** Contrary to Section 133 of the Electronic and Postal Communications Act [Cap 306 R.E. 2022]

**PARTICULARS OF OFFENCE**

**SK**, on 30th May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, did obstruct ..... (Insert name of the person obstructed) to execute .....(insert name of his duties).

OFFENCE			
S. 134 Allowing use of blacklisted phone			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
Any Network service licensees Allows any blacklisted mobile telephones to operate		<ul style="list-style-type: none"><li>- The blacklisted mobile phone</li><li>- The certificate of seizure</li><li>- Statement of the independent witness</li><li>- Statement from TCRA officer</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li></ul>	<ul style="list-style-type: none"><li>- Person to whom directives were issued</li><li>- officer conducted search</li><li>- independent witness (if any)</li></ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**  
**ALLOWING THE USE OF BLACKLISTED PHONE;**  
Contrary to Section 134 of the Electronic and Postal  
Communications Act [Cap 306 R.E. 2022].

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, being .....(insert the title of the authorised Officer and name of Licensee Company) allowed a Blacklisted Mobile Phone.....(insert name of the Mobile phone and its description).

OFFENCE			
S. 135 Tempering with blacklisted phones			
ELEMENT	CLARIFICATION	POSSIBLE EVIDENCE	WITNESS
Physically OR electronically tempers with any blacklisted mobile telephones		<ul style="list-style-type: none"><li>- The blacklisted mobile phone</li><li>- The certificate of seizure</li><li>- Proof of Chain of custody (oral, documentary or any other form)</li><li>- List of blacklisted phones</li></ul>	<ul style="list-style-type: none"><li>- TCRA officer</li><li>officer conducted search</li><li>- independent witness (if any)</li></ul>

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**  
**TEMPERING WITH BLACKLISTED MOBILE**  
**TELEPHONES;** Contrary to Section 135 of the  
Electronic and Postal Communications Act [Cap 306  
R.E. 2022]

**PARTICULARS OF OFFENCE**

**SK**, on diverse dates between 4<sup>th</sup> March, 2017 and 30<sup>th</sup> May, 2019 at Kisasa area within Dodoma District in the Region of Dodoma, tempered with.....(insert the name of MOBILE Telephone tempered and its descriptions)

<b>OFFENCE</b>			
S. 137 (1) , (2) and (3) and 152(1) Sale or possess electronic communication equipment, communication broadcasting apparatus or radio communication equipment without license			
<b>ELEMENT</b>	<b>CLARIFICATION</b>	<b>POSSIBLE EVIDENCE</b>	<b>WITNESS</b>
a) Offer for sale OR sale OR possess for sale Any electronic equipment OR communication broadcasting apparatus		- Electronic equipment /broadcasting apparatus in question - Certificate of seizure - Proof of Chain of custody (oral, documentar	- TCRA officer person conducting the search - Independent witness (if any

Without license	y or any other form)	
b) Possess any radio communication equipment Without license	- Loss report from TCRA (where loss has been occasioned)  Radio communication equipment in question Certificate of seizure Proof of Chain of custody (oral, documentary or any other form)	

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**  
**POSSESSION OF RADIO COMMUNICATION**  
**EQUIPMENT WITHOUT VALID LICENSE; Contrary to**

Sections 137(1) and 152(1) of the Electronic and Postal Communications [Cap 306 R.E. 2022]

### **PARTICULARS OF OFFENCE**

**HAKUNA MATATA** on 30<sup>th</sup> January, 2020 at Kariakoo area within Ilala District in Dar es Salaam Region, was found in possession of Radio Communication Equipment .....(insert name of the Radio equipment) without obtaining License from Tanzania Communications Regulatory Authority.

### **C. OFFENCES UNDER THE MEDIA SERVICES ACT NO. 15 OF 2016**

<b>OFFENCE</b>			
50 (1) Publishing information which is intentionally or recklessly falsified			
<b>Elements</b>	<b>Clarifications</b>	<b>Possible evidence</b>	<b>Witness</b>
- Make use by any means of media service. - For purpose of publishing information which is intentionally or recklessly falsified - In a manner which threatens		- A false information/publication - Proof of media service used - Certificate of Seizure - Proof that information was intentionally or recklessly falsified	- Officer from TCRA - Investigation officer - Officer conducting the search - Independent witness (if any) - A person whose reputation was injured

the interest of defence, public safety, public order, economic interest of the United Republic, public morality or public health; or is injurious to reputation, right and freedom of other person;			
---	--	--	--

**MODEL CHARGE**  
**STATEMENT OF OFFENCE**

**PUBLICATION OF INFORMATION INTENDED TO INJURE REPUTATION:** Contrary to Section 35(1), (2) and 50(1)(a)(ii) of the Media Services Act No. 12 of 2016.

**PARTICULARS OF OFFENCE**

**MAMBO JAMBO**, on 21<sup>st</sup> day of September, 2022 at unknown place within the Region of Dar es Salaam, through his Tiktok account namely **jambo-tz7** did publish edited pictures of his Excellence President of the United Republic of Tanzania **MAISHA NDIO HAYA** with

caption '***RAISI WA MICHONGO***' recklessly to ridicule and injured his reputation.

<b>OFFENCE</b>			
53 Sedition			
<b>Elements</b>	<b>Clarifications</b>	<b>Possible evidence</b>	<b>Witness</b>
<ul style="list-style-type: none"> <li>- Do or attempt to do or makes any preparation to do or conspire with any person to do</li> <li>- Any act or omission with a seditious intention;</li> <li>- Utters any word with seditious intention;</li> <li>- Publishes, sales, offers for sale, distributes or reproduces, any seditious publication;</li> <li>- Imports any seditious publications</li> <li>- Unless he has no reason to believe that it is seditious,</li> </ul>		<ul style="list-style-type: none"> <li>- seditious words</li> <li>- media service used</li> <li>- Certificate of Seizure</li> </ul>	<ul style="list-style-type: none"> <li>- Officer from TCRA</li> <li>- Investigation officer</li> <li>- Officer conducting the search</li> <li>- Independent witness (if any)</li> </ul>