NATIONAL COMPUTER AND CYBERCRIME COORDINATION COMMITTEE

A SECURE CYBERSPACE FOR KENYA AND ITS PEOPLE

INVESTIGATION AND PROSECUTION OF OFFENCES UNDER THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP. 79C

A Rapid Reference Guide

INTEGRITY | JUSTICE | SERVICE

FOREWORD

Information technology has become deeply embedded in the fabric of our society, making cybercrime a persistent and evolving hazard both nationally and globally. Cybercrime is a threat to our national security, malicious actors increasingly exploit the cyberspace to commit crimes, exfiltrate sensitive data, disrupt Critical Information Infrastructure (CIIs) and vital services, orchestrate financial fraud, and undermine public institutions, thereby eroding foundational public trust. Hence the need to hold both State and non-State actors who perpetrate these acts accountable through effective investigations and prosecution.

This Guide is therefore the result of a coordinated partnership involving the National Computer and Cybercrimes Coordination Committee (NC4), the Office of the Director of Public Prosecutions (ODPP) and the National Police Service (NPS).

The Guide provides a detailed breakdown of the various offenses established under the Computer Misuse and Cybercrimes Act (Cap 79C), outlining the specific legal and evidentiary elements required to sustain a criminal charge. Thus, equipping both investigators and prosecutors with the practical tools necessary for effective countering of cybercrime.

As a product of an extensive and inclusive consultative process, this Guide reflects the shared expertise of diverse stakeholders across the criminal justice sector. Securing our cyberspace is fundamental to Kenya's socio-economic development; I therefore urge and encourage all stakeholders to sustain this spirit of cooperation and actively utilize this framework to ensure a safer digital ecosystem for all.

A secure cyberspace for peace, justice and strong institutions.

Dr. Raymond Omollo PhD, CBS,

Principal Secretary State Department of Internal Security and National Administration and the Chairman, National Computer and Cybercrime Coordination Committee.

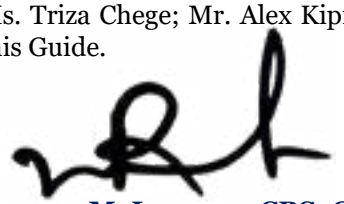
ACKNOWLEDGMENT

Cybercrime poses a unique and dynamic challenge not only to the security of individuals and the nation, but also to the entire criminal justice sector due to its complex and transnational nature. Combating these offenses therefore demands a deeper understanding and coordinated effort among all actors within the criminal justice system.

The Office of the Director of Public Prosecutions (ODPP) plays a pivotal role in this fight by ensuring effective prosecution of cybercrimes. The development of this Guide is both timely and essential for streamlining cybercrime investigations and prosecutions, while serving as a vital capacity-building resource for investigators, prosecutors, and key stakeholders.

I commend the National Computer and Cybercrimes Coordination Committee (NC4) for spearheading the initiative and coordinating the efforts to bring this Guide to fruition. I also extend my gratitude to the National Police Service (NPS) and the ODPP team, without whose vital input this document would not have materialized. The spirit of interagency collaboration exhibited in the making of this Guide is testament to our shared responsibility in countering cybercrime.

This Guide could not have been realized without the relentless efforts, industry and commitment of the technical committee comprising dedicated officers from the respective partner agencies. Special recognition goes to Mr. Vincent Monda, OGW, 'ndc' (K); Mr. Lenkai Shaangwa; Mr. Allen Mulama; Mr. Benson Njagi; Ms. Becky Arunga; Mr. Simon Munene; Mr. Victor Juma Owiti, HSC; Mr. Wesley Nyamache; Mr. Leonard Ngeso; Ms. Lindah Mwamburi; Mr. Willy Momanyi; Mr. Nickson Kinyua, RCrim (K); Mr. Edwin Metto; Mr. Ian Mwau; Mr. Cedric Bett; Mr. Cavin Okoth; Ms. Triza Chege; Mr. Alex Kiprono and Ms. Jennifer Kariuki for the successful development of this Guide.



Renson M. Ingonga, CBS, OGW

Director of Public Prosecutions

MESSAGE FROM THE INSPECTOR GENERAL, NATIONAL POLICE SERVICE (NPS)

The National Police Service (NPS) is mandated to prevent, detect, and investigate crime. The Computer Misuse and Cybercrimes Act (Cap 79C) is one of the primary penal statutes that the NPS is duty-bound to enforce. This enforcement is increasingly critical, as cybercrime now poses the greatest challenge to law enforcement due to its highly complex and transnational nature.

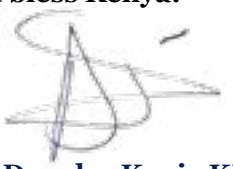
The NPS is typically the first responder to a cybercrime scene. It is critical that these scenes are protected, preserved, and documented to maintain the integrity of vital electronic evidence, which is inherently volatile.

Investigators must secure this integrity through meticulous documentation, identification, packaging, transportation, and storage, while maintaining proper chain of custody records.

It is upon securing the scene and collecting the necessary evidence that investigators compile an investigation file recommending charges to the Director of Public Prosecutions (DPP) for review and direction.

The formulation of this Guide could not have been more timely as it will serve as a quick reference point for investigators and play an instrumental role in the standardization of cybercrime investigations. I commend the multi-agency technical committee for its unwavering efforts and industry in developing this Guide. It will be crucial not only in the fight against cybercrime but also to the overall betterment of service delivery by law enforcement agencies to the citizens of the Republic of Kenya.

God bless Kenya!



Mr. Douglas Kanja Kirocho, MGH, CBS, OGW,

Inspector General of Police, National Police Service

MESSAGE FROM THE DIRECTOR NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE

The rapid digitization of Kenya's public and private sectors has driven both immense economic growth and triggered a corresponding rise in sophisticated cybercrime. Law enforcement officers and prosecutors now face unique technical, legal, and jurisdictional hurdles. Overcoming these challenges requires a deep understanding of digital evidence and seamless, interagency collaboration across the criminal justice system.

In response, the National Computer and Cybercrimes Coordination Committee (NC4), the Office of the Director of Public Prosecutions (ODPP) and the National Police Service (NPS) formed a collaborative partnership to develop this Guide. Serving as a practical toolkit, it bridges the gap between law and operational reality, standardizing evidence management and prosecution strategies nationwide.

I extend my sincere appreciation to the technical committee members from NC4, NPS, and ODPP. Their collective expertise in cybersecurity, investigation and prosecution has greatly enriched this Guide.

Effective cybercrime management requires not only robust laws, but also a shared understanding of operational roles and best practices. I am confident that this Guide will prove invaluable in harmonizing investigations and prosecutions to secure Kenya's digital ecosystem.

Col (Dr) James J. Kimuyu, PhD, 'psc' (K)

Director National Computer and Cybercrimes Coordination Committee

LIST OF ABBREVIATIONS

AG	: Attorney General
AI	: Artificial Intelligence
ARA	: Asset Recovery Agency
BRS	: Business Registration Service
CA	: Communication Authority
CMA	: Capital Markets Authority
CBK	: Central Bank of Kenya
CCTV	: Close Circuit Television
CDR	: Call Data Records
CII	: Critical Information Infrastructure
CMCA	: Computer Misuse and Cybercrimes Act
CSAM	: Child Sexual Abuse Material
DCI	: Directorate of Criminal Investigations
DCS	: Directorate of Children Services
EACC	: Ethics and Anti-Corruption Commission
DPP	: Director of Public Prosecutions
FRC	: Financial Reporting Centre
ISP	: Internet Service Provider
IP	: Internet Protocol
IPOA	: Independent Policing Oversight Authority
IT	: Information Technology
KAA	: Kenya Airports Authority
KPA	: Kenya Ports Authority
KDF	: Kenya Defence Forces
KECIRT/CC	: Kenya Computer Incident Response Team Coordination Centre
KeNIC	: Kenya Network Information Centre
KEBS	: Kenya Bureau of Standards
KIPI	: Kenya Industrial Property Institute
KRA	: Kenya Revenue Authority
MICDE	: Ministry of Information, Communication & the Digital Economy
MLA	: Mutual Legal Assistance
MFA	: Ministry of Foreign Affairs
MNO	: Mobile Network Operators
MoD	: Ministry of Defence
MOINA	: Ministry of Interior and National Administration
MOH	: Ministry of Health
NACOSTI	: National Commission for Science, Technology & Innovation
NRB	: National Registration Bureau
NC4	: National Computer and Cybercrimes Coordination Committee
NCTC	: National Counter Terrorism Centre
NPS	: National Police Service
ODPC	: Office of the Data Protection Commissioner
OTP	: One Time Password
POCAMLA	: Proceeds of Crime and Anti Money Laundering Act
P3 FORM	: Police Form 3
SACCO	: Savings and Credit Cooperative Organization
VA	: Virtual Asset
VASP	: Virtual Asset Service Provider
WPA	: Witness Protection Agency

DEFINITION OF TERMS[1]

S/No	Term	Definition
1.	**Attribution**	The act of assigning a cause, credit, or origin to something.
2.	**Child Sexual Abuse Material (CSAM)**	Any visual depiction, such as photographs, videos, or computer-generated imagery, that shows a child involved in sexually explicit conduct or depicted in a sexual context.
3.	**Internet**	A global system of billions of interconnected computers and electronic devices that communicate with one another.
4.	**Internet Protocol (IP) address**	A unique numerical label assigned to every device connected to a computer network.
5.	**Call Data Records (CDR)**	A standardized data file or log generated by telecommunication switches. It captures metadata about a call or data session, such as originating/terminating numbers, timestamps, and duration. Importantly, it does not contain the actual voice content.
6.	**Critical data**	Highly sensitive, classified, or proprietary information that, if stolen or manipulated, grants the attacker a strategic, economic, military, or political advantage
7.	**Critical database**	A high-value repository containing sensitive information that, if compromised, stolen, or monitored, gives a threat actor (such as a nation state or corporate spy) a distinct strategic, political, military, or economic advantage

Terms specifically defined in the CMCA or other statutes have not been specifically included in this Guide. Users are therefore advised to refer to the various enabling provisions of law for any terminology of interest.

TABLE OF CONTENTS

CHAPTER I: UNDERSTANDING CYBERCRIMES

CHAPTER I

UNDERSTANDING CYBERCRIMES

1.0 Introduction

The rapid digitization of Kenya's public and economic sectors has fundamentally shifted the domestic criminal landscape. Traditional crimes have evolved, and entirely new vectors of criminality have emerged, demanding a modernized approach to criminal justice. To effectively combat these threats, the Computer Misuse and Cybercrimes Act, Cap 79C (CMCA) was enacted to provide for offences relating to computer systems.

At its core, the CMCA aims to protect the confidentiality, integrity, and availability of computer systems, programs, and data, while actively providing the legal mechanisms necessary for the timely prevention, detection, investigation, and prosecution of cyber offences. Understanding cybercrime therefore requires a clear grasp of how criminals leverage technology to perpetrate various offences.

1.1 Characteristics of Cybercrime

Although there is no universally accepted definition of cybercrime, the CMCA defines cybercrime as an offence committed through the use of information and communication technology to target networks, systems, data; websites or technology or to facilitate a crime. Regardless of how cybercrime is defined it is perhaps easier to identify some of its characteristics:

i. **Scale:** The large number of persons using the internet and related communications means that the potential number of victims and offenders is immense. Criminals' use of computer technology lets them commit crime on a scale far exceeding what is possible in the real world.

ii. **Accessibility:** The internet continues to reach areas of the world that it has not traditionally been found and this is particularly true where there is access to both mobile technology and broadband internet. This provides opportunities for offenders to meet like-minded persons.

iii. **Anonymity:** The use of computer technology has made it possible to mask one's identity thereby making it difficult to identify and apprehend those responsible for cybercrimes.

iv. **Volatility of data:** Electronic data is susceptible to erasure and distortion which has made data more fragile, easily degradable and prone to dissipation.

v. **Global reach:** The transnational nature of cybercrime poses significant challenges to investigators where the evidence exists outside Kenya's jurisdiction.

1.2 Overview of the Computer Misuse and Cybercrimes Act

The CMCA establishes a comprehensive legal framework designed to protect the confidentiality, integrity, and availability of computer systems, programs, and data, while facilitating the efficient detection, prevention, and prosecution of cybercrimes. At its administrative core, the Act establishes the National Computer and Cybercrimes Coordination Committee (NC4) to coordinate national cybersecurity strategies, manage cyber threat responses and oversee the implementation of cybersecurity standards across public and private sectors. A pivotal function of the NC4 under the framework is the power to designate specific digital networks and systems operating in sectors delienated under the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024, as Critical Information Infrastructure (CII). Such designation results in subjecting their operators to stringent auditing, risk assessment, and mandatory 24-hour breach reporting timelines.

Substantively, the Act criminalizes a broad spectrum of misconduct in cyberspace. It establishes penalties for offences like unauthorised access (hacking), unauthorised interference, and illegal interception of data streams. Additionally, it targets personal and financial harms by penalizing phishing, identity theft, computer fraud, cyber harassment, and the distribution of intimate images without consent. The Act also explicitly outlaws cyber espionage and cyber terrorism, imposing heavy fines and imprisonment for acts that compromise state security or target national Critical Information Infrastructure.

To ensure effective enforcement, the Act empowers law enforcement with specialized investigative tools, detailing the legal mechanisms for court-authorised search and seizure of electronic data, production orders, and the expedited preservation and disclosure of traffic and content data by service providers. Recognizing the transnational nature of cybercrimes, the CMCA includes robust provisions for international cooperation, anchoring extraterritorial jurisdiction and mutual legal assistance frameworks to facilitate cross border data preservation and extradition.

Furthermore, the Act significantly escalate the state's intervention capabilities and penal structural accountability by introducing judicial options for content removal and system deactivation when platforms or devices are proven to promote unlawful activities, electronic child exploitation, or religious extremism and cultism (Section 46A).

Through this integrated approach of institutional oversight, precise criminalization, and adaptive enforcement powers, the CMCA stands as the cornerstone of Kenya's digital rule of law and national cyber resilience.

1.3 Justification, Objectives and Scope of this Guide

Successful investigation and prosecution of cybercrimes demand absolute clarity on substantive law and procedural fairness. Central to this is the need to standardize and streamline the entire lifecycle of a cybercrime file from investigation to prosecution. This Guide outlines the offences under the CMCA structured template charges, material elements, and the relevant agencies to be engaged for effective investigation and prosecution. Furthermore, the Guide actively streamlines the procedural framework for cybercrime investigations by providing standardized template applications for vital investigative steps.

Crucially, all investigation files realting to the offences under the CMCA must be accompanied by a duly signed Certificate of Electronic Evidence pursuant to Section 106B of the Evidence Act (Cap 80). Additionally, a signed Certificate of Translation must accompany any piece of evidence not rendered in English or Swahili. Finally, to maintain a flawless chain of custody, the investigation file must contain the specific court orders authorizing each investigative step taken to retrieve the digital evidence relied upon.

The Guide is designed to assist investigators and prosecutors in navigating the complexities of cybercrimes strictly as an operational aid. Therefore, it should not be taken as a substitute for statutory provisions, binding judicial precedents, or comprehensive independent legal research.

1.4 Virtual Assets and Cybercrime

The rapid digitization of the global financial system has created a paradigm shift in the criminal landscape, primarily driven by the proliferation of virtual assets (VAs). While VAs offer advantages in transaction speed, reduced cross-border friction, and financial inclusion, their inherent structural characteristics; specifically pseudo-anonymity, rapid peer-to-peer transferability, and decentralization, have simultaneously transformed them into highly attractive instruments for modern criminal syndicates.

The Kenya Virtual Assets Service Providers Act, 2025 provides the legal framework to license and regulate the activities of virtual asset service providers. It provides a tripartite integration of the CMCA, the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), and the Virtual Asset Service Providers (VASP) Act in dealing with virtual assets related offences.

In the context of cybercrime, virtual assets occupy a dual position: they operate symmetrically as both a primary target of cyber threats and the financial enabling vehicle for commission of cybercrimes. The CMCA broadens the definition of an asset to encompass virtual property, thereby providing a pathway to charge threat actors with computer fraud, unauthorized system access, or data interference when digital wallets and smart contracts are compromised. Concurrently, the Proceeds of Crime and Anti Money Laundering Act (POCAMLA) treats illicitly acquired virtual assets as proceeds of crime. Hence, granting specialized bodies like the Asset Recovery Agency (ARA) the judicial mandate to trace, freeze, and ultimately forfeit VAs. Ultimately, effective cybercrime prosecution extends beyond establishing a system breach; it demands the swift tracking, preservation and forfeiture of the proceeds of crime.

1.5 Technology-Facilitated Offences

The Computer Misuse and Cybercrimes Act (Cap 79C) provides a robust framework for prosecuting traditional crimes committed through the use of a computer system. Under Section 46 of the Act, any person who perpetrates an offence under any other law using a computer system commits a distinct offence under the CMCA, carrying a penalty equivalent to that of the underlying crime.

Furthermore, Section 47 explicitly extends all investigative powers and procedures of the Act to technology facilitated offences. This ensures that the specialized mechanisms for collecting, preserving, and presenting electronic evidence apply uniformly; whether an offence is explicitly defined under the CMCA or established under any other written law.

When dealing with technology facilitated offences, investigators are required to conduct investigations that not only prove the underlying offence but also outline the manner in which a computer system was exploited to aid in perpetrating the offence. This dual focus is critical for sentencing.

Pursuant to Section 46 of the Computer Misuse and Cybercrimes Act (CMCA), where a crime under any other statute is committed through the instrumentality of a computer system, the court is empowered to impose an additional or enhanced sentence. In determining sentence severity under Section 46(2), judicial officers are statutorily mandated to evaluate key aggravating factors arising from digital exploitation. These include assessing the degree to which digital technology amplified the **scale** and **impact** of the offence, the total number of victims affected, and whether the criminal conduct yielded commercial advantage or significant financial gain. Furthermore, the court weighs the pecuniary value of the consequential loss or damage, the presence of any breach of trust or professional duty, the overall conduct of the accused person, and any other aggravating circumstances relevant to the interests of justice.

By leveraging this Guide, investigators and prosecutors can ensure efficient effective and just outcomes in cybercrime prosecution.

CHAPTER II:
LEGAL AND INSTITUTIONAL FRAMEWORK IN THE INVESTIGATION AND PROSECUTION OF CYBERCRIMES IN KENYA

CHAPTER II

LEGAL AND INSTITUTIONAL FRAMEWORK IN THE INVESTIGATION AND PROSECUTION OF CYBERCRIMES IN KENYA

2.0 Legal Framework

Cybercrime investigation and prosecution in Kenya operate within the broader context of Kenya's criminal justice system, anchored primarily in the Constitution of Kenya, 2010. The enforcement of the CMCA relies on general principles of substantive criminal law. This requires proving both the physical act (actus reus) and the requisite mental state (mens rea) beyond a reasonable doubt just as it is in other criminal cases. Similarly, general principles of criminal liability and common intention governed by the Penal Code (Cap 63)—apply equally to computer and cybercrimes.

The Computer Misuse and Cybercrimes Act provides the core substantive and procedural framework for investigating and prosecuting cybercrimes in Kenya. However, statutory powers under the Act do not operate in a legal vacuum; constitutional compliance remains mandatory at every stage of enforcement. Consequently, every investigative step and prosecutorial decision must strictly uphold fundamental rights and freedoms, ensuring that any statutory limitation imposed fully meets the justification criteria set out under Article 24 of the Constitution.

2.1 Legal Instruments

The following legal instruments are crucial in the prosecution of computer and cybercrimes in Kenya:

2.1.1 The Evidence Act, Cap 80

The Evidence Act (Cap 80) governs the law of evidence in Kenya, providing the statutory foundation for admissibility of digital evidence. Section 78A provides for the admissibility of digital and electronic evidence, while Section 106B provides the admissibility criteria of electronic records and computer output. Section 106B sets out conditions to verify device reliability, data generation integrity, and custody logs. A valid Certificate of Electronic Evidence under Section 106B, signed by a person responsible for managing the relevant device or activity, is a mandatory requirement for admissibility of electronic and digital evidence.

2.1.2 The Criminal Procedure Code,Cap 75

The Criminal Procedure Code, Cap 75 governs procedural conduct across all criminal prosecutions in Kenya. It establishes the legal parameters for executing arrests, obtaining search warrants, drafting charge sheets, determining bail and bond, and conducting trials. Consequently, where the Computer Misuse and Cybercrimes Act (CMCA) lacks specific procedural mechanisms, the Criminal Procedure Code acts as the supplementary statute.

2.1.3 The Data Protection Act, Cap 411C

The Data Protection Act, Cap 411C regulates the processing of personal data, setting out the fundamental rights of data subjects alongside the obligations of data controllers and processors. Because cybercrime investigations and prosecutions inevitably involve collecting, handling, and analyzing vast amounts of personal data, law enforcement agencies must ensure that all digital evidence and personal information are managed in compliance with the principles established under the Data Protection Act.

2.1.4 The Kenya Information and Communication Act, Cap 411A

The Kenya Information and Communication Act, Cap 411A regulates telecommunication service providers, mobile network operators, SIM card registration, and domain name registries. It establishes the statutory framework under which investigators request subscriber information,

Call Data Records (CDRs), and IP address allocation histories. Furthermore, the Communications Authority established under the Act, hosts the national Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), which serves as the critical operational liaison between law enforcement agencies, Internet Service Providers (ISPs), and international social media platforms.

2.1.5 The Mutual Legal Assistance Act, Cap 75A

The Mutual Legal Assistance Act, Cap 75A provides the legal framework for Kenya to request and offer assistance in criminal investigations, prosecutions, and judicial proceedings involving foreign jurisdictions. Given the inherently transnational nature of cybercrime, the Mutual Legal Assistance Act governs formal cross-border cooperation. The Act regulates the issuance of diplomatic requests, the execution of Letters of Request (Letters Rogatory), and the lawful acquisition of admissible extraterritorial digital evidence.

2.1.6 The Prevention of Terrorism Act, Cap 59B

The Prevention of Terrorism Act, Cap 59B provides legal measures for detecting, preventing, and prosecuting terrorist activities in Kenya. To maintain harmony across national security legislation, Section 33 of the Computer Misuse and Cybercrimes Act (CMCA), which criminalizes cyberterrorism, explicitly imports the definition of a "terrorist act" as assigned under Section 2 of the Act. Consequently, where computer systems are used to facilitate or execute terrorist acts, investigators and prosecutors should apply the substantive standards and procedural provisions set out under the Prevention of Terrorism Act alongside the CMCA.

2.1.7 The Proceeds of Crime and AntiMoney Laundering Act,Cap 59A

The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), Cap 59B provides the statutory framework for detecting, preventing, and penalizing money laundering, as well as identifying, tracing, freezing, seizing, and forfeiting the proceeds of crime. Cybercrime is predominantly a predicate offence for money laundering. Therefore, prosecutors must proactively seek preservation and forfeiture orders where necessary. Complementing this framework, Section 44 of the Computer Misuse and Cybercrimes Act (CMCA) explicitly empowers the court to order the confiscation and forfeiture of monies, proceeds, and assets derived from or acquired through computer and cybercrimes. Directing that such recovery be conducted in alignment with POCAMLA mechanisms.

2.1.8 The Virtual Assets Service Providers Act, 2025

The Virtual Asset Service Providers (VASP) Act, 2025 establishes the regulatory, licensing, and supervisory framework for entities offering virtual asset services, such as cryptocurrency exchanges, custodial wallet providers, and digital token issuers, operating in or from Kenya. The VASP Act complements Section 2 of the Computer Misuse and Cybercrimes Act (CMCA), which defines assets to include virtual assets and digital representations of value. Because cybercriminals routinely utilize virtual assets to launder illicit proceeds, the VASP Act equips investigators and prosecutors with critical mechanisms to:

i. Enforce Know-Your-Customer (KYC) and Anti-Money Laundering (AML) audit trails across platforms regulated by the Central Bank of Kenya (CBK) and Capital Markets Authority (CMA);

ii. Apply for preservation and forfeiture orders for virtual assets, track transaction histories across virtual asset wallets and exchange ledgers; and

iii. Hold non-compliant or unlicensed service providers criminally liable.

2.1.9 The Victim Protection Act, Cap 79A

The Victim Protection Act (Cap 21A) codifies the rights and welfare of victims of crime throughout the criminal justice process. Given that computer and cybercrimes might inflict severe emotional, reputational or economic harm, investigators and prosecutors are required to enforce the protection mechanisms under the Victim Protection Act. Specifically, law enforcement should safeguard victim dignity, physical safety, and data privacy during digital evidence handling and testimony, deploy protective measures for vulnerable victims (such as in-camera proceedings or identity masking), and proactively submit Victim Impact Statements while applying for court-ordered compensation, restitution, and reparations during sentencing pursuant to Section 45 of the Computer Misuse and Cybercrimes Act.

2.2 Institutional Framework

The effective detection, investigation, and prosecution of cybercrimes under the Computer Misuse and Cybercrimes Act (CMCA) rely upon a multi-agency institutional framework designed to bridge the gap between technology, national security, and criminal justice. At the core of this framework is the National Computer and Cybercrimes Co-ordination Committee (NC4), established under Part II of the CMCA as the apex entity for cybersecurity governance, threat management, and policy formulation. Comprising key state organs with distinct statutory mandates, this coordinated framework provides a clear operational structure for countering cybercrime across Kenya.

This section outlines some critical institutions and their specific roles in the cybercrime investigation and prosecution lifecycle.

2.2.1 The National Computer and Cybercrimes Coordination Committee (NC4)

The National Computer and Cybercrimes Coordination Committee (NC4), established pursuant to Section 4 of the Computer Misuse and Cybercrimes Act, is the primary multi-agency body responsible for national cybersecurity policy, strategic coordination, and operational oversight. NC4 unites key national security, intelligence, and justice sector agencies to formulate national cybersecurity strategies, monitor digital threat landscapes, and manage Critical Information Infrastructure (CII). Operationally, NC4 acts as the focal point for threat intelligence and cybersecurity incident reporting, harmonizing cross-agency responses and issuing technical advisories. For investigators and prosecutors, NC4 provides overarching policy direction, facilitates inter-agency cooperation, and establishes standardized operational protocols for managing complex, multi-sector cyber incidents.

2.2.2 The Office of the Director of Public Prosecutions (ODPP)

The Office of the Director of Public Prosecutions (ODPP) holds the sole constitutional authority under Article 157 of the Constitution to direct criminal investigations and provide prosecution services. Prosecutors review police files to evaluate the sufficiency of evidence, guide investigators and undertake prosecution of computer and cybercrimes. Additionally, the ODPP coordinates applications seeking freezing, preservation, and forfeiture of assets pursuant to Section 44 of the CMCA and the enabling provisions of POCAMLA, while ensuring victim rights are safeguarded pursuant to the Victim Protection Act.

2.2.3 The National Police Service (NPS)

The National Police Service, established pursuant to Article 243 of the Constitution of Kenya, is the law enforcement agency charged with detecting, preventing, and investigating cybercrimes. Through the Directorate of Criminal Investigation (DCI) the NPS carries out investigations and evidence management. Forensic examiners from the DCI are tasked with maintaining chain of custody, generating cryptographic hash values, and executing forensic extractions to guarantee admissible digital evidence in compliance with court orders.

2.2.4 The Communications Authority of Kenya (CA)

The Communications Authority of Kenya (CA), established pursuant to Section 3 of the Kenya Information and Communication Act, is the statutory regulator for the telecommunications, broadcasting, and postal sectors. Housed within the CA is the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC), which functions as Kenya's operational national point of contact for cybersecurity incidents. For law enforcement, the CA serve as vital operational bridges to telecommunications operators, mobile network service providers, domain registries, and international tech platforms, facilitating the lawful acquisition of subscriber details, Call Data Records (CDRs), and IP allocation logs.

2.2.5 The Judiciary of Kenya

The Judiciary of Kenya serves as the ultimate constitutional safeguard and arbiter in the administration of justice. In cybercrime enforcement, the courts perform a critical dual role: providing judicial preauthorization for investigations and adjudicating criminal prosecutions. The courts scrutinize miscellaneous applications to ensure compliance with constitutional rights before granting search warrants, digital device seizure orders, real time data interception, and production orders under the CMCA. Additionally, the Judiciary plays a central role in cross-border enforcement by issuing transmission orders under the Mutual Legal Assistance Act (Cap 75A). During trial, judicial officers evaluate the admissibility of digital output under Section 106B of the Evidence Act, weigh expert forensic testimony, oversee asset freezing and forfeiture proceedings under Section 44 of the CMCA, and enforce victim restitution and compensation under Section 45 of the CMCA.

2.2.6 Office of the Attorney General

The Office of the Attorney General, established pursuant to Article 156 of the Constitution of Kenya, serves as the principal legal advisor to the National Government and plays a pivotal structural role in facilitating international judicial cooperation. Designated under Section 5 of the Mutual Legal Assistance Act (Cap 75A) as the Central Authority for Kenya, the Attorney General's office is the exclusive diplomatic and legal conduit for processing cross-border requests in criminal matters. The Attorney-General transmits and receives outgoing and incoming requests for legal assistance, oversees the execution of Letters Rogatory, and ensures that foreign evidentiary requests comply with domestic law and international treaties.

The following table is a summary of some of the critical institutions in cybercrime investigations and prosecutions:

S/No	AGENCY	ROLE
1	**National Computer and Cybercrimes Coordination Committee (NC4)**	Central coordinating body for all CMCA offences; first point of contact for CII compliance, cyber-threat reports and inter-agency coordination.
2	**National Police Service (NPS)**	Primary investigative agency charged with investigating cybecrimes.
3	**Office of the Director of Public Prosecutions (ODPP)**	Conducting prosecution of cybercrimes
4	**Asset Recovery Agency (ARA)**	Tracing, freezing, forfeiture and management of proceeds of crime.

5	**Financial Reporting Centre (FRC)**	A financial intelligence unit that assist in the identification of the proceeds of crime and combating money laundering, terrorism financing and proliferation financing.
6	**Central Bank of Kenya (CBK)**	Principal regulator of banks, digital payment systems Virtual Asset Service Providers and other relevant financial institutions.
7	**Capital Markets Authority (CMA)**	Principal institution responsible for regulating and developing an orderly, fair and efficient capital markets in Kenya.
8	**Office of the Data Protection Commissioner (ODPC)**	Principal institution for regulating the processing of personal data and enforcement of the Data Protection Act.
9	**Communications Authority of Kenya (CA)**	Principal regulatory agency with regulatory oversight over the provision of telecommunications, radio communications, broadcasting, electronic transactions, the country's numbering and frequency spectrum resources as well as postal and courier services.
10	**Mobile Network Operators (MNOs)**	Telecommunication companies that provide various services including wireless voice, text, mobile money and data services.
11	**Virtual Asset Service Providers (VASPs)**	Companies that carry on the business of virtual asset services.
12	**Directorate of Children Services (DCS)**	State department charged with the mandate of safeguarding the rights and promoting the welfare of all children in Kenya.
13	**National Commission for Science, Technology and Innovation (NACOSTI)**	Principal institution charged with regulating and quality assurance in the science, technology and innovation sector.
14	**Ministry of Defence (MoD)**	Government ministry charged with defending and protecting the sovereignty and territorial integrity of the Republic of Kenya.
15	**Ministry of Health (MoH)**	Government ministry charged with coordinating and regulating healthcare services, healthcare service providers, health products and health technologies.
16	**National Counter Terrorism Centre (NCTC)**	A multi-agency institution charged with coordinating national counter-terrorism measures that prevent, detect, deter and disrupt terrorism acts.
17	**Witness Protection Agency (WPA)**	Principal agency charged with protection of witnesses in criminal cases and other proceedings.

CHAPTER III: CYBERCRIMES, ESSENTIAL INGREDIENTS AND EVIDENCE REQUIRED

CHAPTER III

CYBERCRIMES, ESSENTIAL INGREDIENTS AND EVIDENCE REQUIRED

This chapter outlines the offences under the CMCA alongside their equivalent descriptions, material elements, and the relevant agencies to be engaged for effective investigation and prosecution. The list provided below is not exhaustive and is a general guide which should be adapted to suit the unique circumstances of each case.

3.1 Offences Relating to Auditing of Critical Information Infrastructures

3.1.1 Failure to File a Compliance Report/ Failure to Cooperate with an Audit on a Critical Information Infrastructure

Section	**13 (5) (a)**
Description	An owner or authorised person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person fails to file a compliance report and fails to cooperate with an audit to be performed on a critical information infrastructure to evaluate compliance with the directives issued
Actus reus	▪ Failing to file a compliance report ▪ Failure to cooperate with an audit
Mens rea	▪ Knowledge of the audit ▪ Knowledge that the compliance report is due
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State;
	▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or an authorised person in control of a CII; ▪ Proof of failure to file a compliance report; ▪ Proof of failure to cooperate with an audit; ▪ Proof that the compliance report is due.
Relevant agency	NC4, NPS or any other relevant agency.
General remarks	Knowledge can be inferred as this is a statutory requirement for all designated CIIs

3.1.2 Failure to Provide Additional Information to the Director National Computer and Cybercrimes Coordination Committee

Section	13 (5) (b)
Description	An owner or authorised person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person fails to provide to the Director such additional information as may be necessary within a specified period to evaluate the report of an audit in line with the critical infrastructure after he or she has been requested to do so to the Director;
Actus reus	Failure to provide the Director NC4 with additional information
Mens rea	Knowledge of the request for additional information by the Director NC4
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State; ▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or an authorised person in control of a CII; ▪ Proof of demand for additional information by the Director NC4; ▪ Proof of service of the request for additional information by the Director NC4; ▪ Proof of lapse of the time for giving the additional information requested.
Relevant agency	NC4, NPS or any other relevant agency.
General remarks	Knowledge of the existence of the demand for additional information can be inferred from proof that the demand was duly served upon the CII.

3.1.3 Hindering, Obstructing or Attempting to Influence a Member of the National Computer and Cybercrimes Coordination Committee/ Person/ Entity

Section	13 (5) (c)
Description	An owner or authorised person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person hinders, obstructs or improperly attempts to influence any member of the Committee, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit.
Actus reus	Obstruction/ hindering/ attempting to influence any member of NC4, entity or person
Mens rea	Knowledge that the member of NC4, entity or person was monitoring, evaluating and reporting on the adequacy and effectiveness of an audit of the CII
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State;
	▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or an authorized person in control of a CII;
	▪ Proof of notification that any member of NC4, entity, or person would monitor, evaluate and report on the adequacy and effectiveness of an audit of the CII; ▪ Proof of obstruction/ hindering or attempting to influence any member of NC4, entity or person; ▪ Proof that the obstruction/ hindering or attempt to influence was in respect to monitoring/ evaluation and reporting on the adequacy and effectiveness of an audit of the CII.
Relevant agency	NC4, NPS or any other relevant agency.
General remarks	Knowledge that the member of NC4, entity or person was monitoring, evaluating and reporting on the adequacy and effectiveness of an audit of the CII would be inferred from proof that the CII was notified of the intended act.

3.1.4 Hindering, Obstructing or Attempting to Influence Authorized Person

Section	13 (5) (d)
Description	An owner or authorised person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person hinders, obstructs or improperly attempts to influence any person authorized to carry out an audit
Actus reus	Hindering, obstructing or improperly attempting to influence any person authorized to carry out an audit
Mens rea	▪ Knowledge that the person is authorized to carry out an audit of the CII ▪ Knowledge that the CII is to be audited
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State; ▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or authorized person in control of a CII; ▪ Proof of hindering/ obstruction or attempting to influence a person authorized to carry out an audit; ▪ Proof of notification to the CII that an audit would be undertaken; ▪ Proof that the person is authorized to carry out an audit.
Relevant agency	NPS NC4 or any other relevant agency.
General remarks	Knowledge that the CII is to be audited can be inferred from the notification to the CII that an audit would be undertaken

3.1.5 Failure to Cooperate with Authorized Person

Section	13 (5) (e)
Description	An owner or authorized person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person fails to co-operate with any person authorized to carry out an audit
Actus reus	Failing to cooperate with any person authorized to carry out an audit
Mens rea	Knowledge that the CII was to be audited
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State; ▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or authorized person in control of a CII; ▪ Proof of failure to cooperate with a person authorized to carry out an audit; ▪ Proof that the person is authorized to carry out an audit; ▪ Proof of notification to the CII that an audit would be undertaken.
Relevant agency	NPS, NC4 or any other relevant agency.
General remarks	Knowledge that the CII was to be audited can be inferred from proof of notification to the CII that an audit would be undertaken

3.1.6 Failure to Assist or Provide Technical Assistance or Support to Authorized Person

Section	13 (5) (f)
Description	An owner or authorized person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person fails to assist or provide technical assistance and support to a person authorized to carry out an audit.
Actus reus	Failure to assist or provide technical assistance and support to a person authorized to carry out an audit
Mens rea	Knowledge that the CII was required to assist/ provide technical assistance/ support to the authorized person undertaking the audit.
Evidence	▪ Proof that the facility, system, network or process is a CII pursuant to Section 2 of the CMCA; ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a debilitating impact on the availability, integrity or delivery of essential services; or ▪ Proof that the facility, system, network or process is one whose incapacity, destruction or modification would have a significant impact on national security, national defense, or the functioning of the State; ▪ Proof that the facility, system, network or process renders services that fall within the critical services pursuant to the second schedule of the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024; ▪ Proof that the suspect is an owner or authorized person in control of a CII ▪ Proof of failure to provide technical assistance to a person authorized to carry out an audit; ▪ Proof that the person is authorized to carry out an audit; ▪ Proof of notification to the CII that an audit would be undertaken; ▪ Proof that the CII was notified of the need to provide technical assistance and support to the authorized person undertaking the audit.
Relevant agency	NPS, NC4 or any other relevant agency.
General remarks	Review the content of the notification to CII to establish that it expressly required the CII to assist or provide technical assistance and support to the authorized person undertaking the audit

3.2 Offences Relating to Unauthorised Access to a Computer System

3.2.1 Unauthorised Access

Section	Section 14 (1)
Description	A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Causing a computer system to perform a function by infringing security measures without authority or consent
Mens rea	▪ Knowledge that such access is unauthorised/unconsented to; and ▪ Intention to gain access by bypassing security measures
Evidence	▪ Proof of existence of a computer system; ▪ Proof of ownership or control of the computer system which has been accessed without authority. (e.g documentation on ownership/control; ▪ Proof that the computer system was accessed by infringing security measures; ▪ Proof that the access to the computer system was unauthorized; ▪ Proof that the suspect is linked to the unauthorized access; ▪ Proof of lawful acquisition of evidence e.g. Court orders authorising search, seizure, or exploration, or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant Agency	AG, NPS, ISPs, Judiciary, CA, MNOs, NACOSTI, NC4, ODPC, CBK, CMA, VASPs or any other relevant agency.
General remarks	The prosecution should prove not only how the system was accessed, but also the absence of authority at the exact moment of intrusion.

3.2.2 Unauthorised Access with Intent to Commit Further Offence

Section	Section 15 (1)
Description	A person who commits an offence under section 14 with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person, commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	Infringing security measures to cause a computer system to perform a function without authority or consent.

Mens rea	▪ Knowledge that such access is unauthorised/unconsented to; ▪ Intention to gain access by infringing security measures; ▪ Intention to commit a further offence under any Kenyan law;
Evidence	▪ Evidence of existence of a computer system; ▪ Proof of ownership or control of the computer system which has been accessed without authority. (e.g documentation on ownership/ control; ▪ Proof that the computer system was accessed by infringing security measures; ▪ Proof that the access to the computer system was unauthorized; ▪ Proof of facilitation/ preparation/ commission of a further offence; ▪ Proof of intention to commit a further offence under any Kenyan law; ▪ Proof that the suspect is linked to the unauthorized access; ▪ Proof of lawful acquisition of evidence: Court orders authorising search, seizure, and exploration, or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NACOSTI, Judiciary, NC4, ODPC, CA, AG, CBK, CMA, VASPs, ISPs, MNOs or any other relevant agency.
General remarks	The further offence need not be a cybercrime as long as it is an offence under Kenyan law.

3.3 Offences Relating to Unauthorised Interference to a Computer System, Program or Data

3.3.1 Unauthorised Interference

Section	**Section 16 (1)**
Description	A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	▪ Doing any act that causes an unauthorized interference to a computer system, program, or data. ▪ The impairment of the confidentiality, integrity, or availability of the system, program, or data
Mens rea	▪ Intention to commit any act causing unauthorised interference; and ▪ The act was done without authority or consent

Evidence	▪ Proof of existence of a computer system, program or data; ▪ Proof of interference to a computer system, program or data; ▪ Proof that the interference to the computer system, program or data was unauthorized; ▪ Proof that the suspect is linked to the unauthorized interference; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, NACOSTI, Judiciary, CA, ODPC, MNO's, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	Always establish a clear link between the suspect's input and the system's failure. The forensic report should clearly demonstrate that the system did not suffer a random technical glitch or routine hardware failure, but rather a direct, intentional disruption triggered by the suspect's unauthorized actions.

3.3.2 Unauthorised Interference Resulting in a Significant Financial Loss

Section	**Section 16 3 (a)**
Description	A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, which results in a significant financial loss to any person; commits an offence and is liable on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Conduct causing an unauthorised interference ▪ Impairing the confidentiality, integrity or availability of a computer system, program or data ▪ Significant financial loss
Mens rea	▪ Intention to commit any act causing unauthorised interference; and ▪ Lack of authorisation
Evidence	▪ Proof of existence of a computer system, program or data; ▪ Proof of interference to a computer system, program or data; ▪ Proof of significant financial loss resulting from the unauthorized interference to a computer system, program or data; ▪ Proof that the interference to the computer system, program or data was unauthorized; ▪ Proof that the suspect is linked to the unauthorized interference; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data;

	▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act;
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, VASPs, CBK, CMA, Financial Institutions, FRC, ARA, ISPs or any other relevant agency.
General remarks	• The investigation file should quantify both *direct losses* (e.g., funds fraudulently diverted, cost of replacing destroyed hardware, forensic consultant fees to restore the system) and *consequential losses* (e.g., revenue lost during business interruption). Investigators should secure all corresponding invoices, audit reports, and bank statements to substantiate this figure. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.3.3 Unauthorised Interference which Threatens National Security

Section	**Section 16 (3) (b)**
Description	A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, which threatens national security; commits an offence and is liable on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Conduct causing unauthorised interference ▪ Impairing the confidentiality, integrity or availability of a computer system, program or data ▪ Threat to national security
Mens rea	▪ Intention to commit any act causing unauthorised interference ▪ Lack of authorization
Evidence	▪ Proof of existence of a computer system, program or data; ▪ Proof of interference to a computer system, program or data; ▪ Proof of credible threat to national security resulting from the unauthorized interference to a computer system, program or data; ▪ Proof that the interference to the computer system, program or data was unauthorized; ▪ Proof that the suspect is linked to the unauthorized interference; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs, MoD or any other relevant agency.
General remarks	Prosecutors may secure closed-court sessions (*in-camera*) or redacted evidence orders to avoid compromising classified security operations or State secrets that may further undermine national security.

3.3.4 Unauthorized Interference which Causes Physical Injury or Death to any Person

Section	Section 16 (3) (c)
Description	A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, which causes physical injury or death to any person; commits an offence and is liable on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Conduct causing unauthorised interference ▪ Impairing the confidentiality, integrity or availability of a computer system, program or data ▪ Physical injury or death of a person
Mens rea	▪ Intention to commit any act causing unauthorised interference; and ▪ Lack of authorization
Evidence	▪ Proof of existence of a computer system, program or data; ▪ Proof of interference to a computer system, program or data; ▪ Proof of physical injury or death to any person resulting from the unauthorized interference to a computer system, program or data; ▪ Proof that the interference to the computer system, program or data was unauthorized; ▪ Proof that the suspect is linked to the unauthorized interference; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, MoH, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	• The investigation file should contain evidence that directly links the resultant physical injury or death to the unauthorized intereference to a computer system, program or data. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.3.5 Unauthorised Interference which Threatens Public Health or Public Safety

Section	Section 16 (3) (d)
Description	A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, which threatens public health or public safety; commits an offence and is liable on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

Actus reus	▪ Conduct causing unauthorised interference ▪ Impairing the confidentiality, integrity or availability of a computer system, program or data ▪ Threat to public health or public safety
Mens rea	▪ Intention to commit any act causing unauthorised interference; and ▪ Lack of authorisation
Evidence	▪ Proof of existence of a computer system, program or data; ▪ Proof of interference to a computer system, program or data; ▪ Proof of credible threat to public health or public safety resulting from the unauthorized interference to a computer system, program or data; ▪ Proof that the interference to the computer system, program or data was unauthorized; ▪ Proof that the suspect is linked to the unauthorised interference; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act,
Relevant agency	NC4, NPS, MoH, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs, MoD or any other relevant agency.
General remarks	The investigation file should contain evidence that directly links the resultant credible threat to public health or public safety to the unauthorized intereference to a computer system, program or data.

3.4 Offences Relating to Unauthorised Interception
3.4.1 Unauthorised Interception

Section	**Section 17 (1)**
Description	A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	▪ Monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data ▪ Causing transmission of data to or from a computer system over a telecommunication system
Mens rea	▪ Intention to intercept or cause data to be intercepted; and ▪ Lack of authorisation

Evidence	▪ Proof of existence of a telecommunication system; ▪ Proof of existence of a computer system; ▪ Proof of intention to intercept data or cause data to be intercepted from a computer system over a telecommunication system without authority; ▪ Proof of monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Proof of conduct causing transmission of data to or from a computer system over a telecommunication system; ▪ Proof of ownership/ control of the computer system from which unauthorized interception occurs; ▪ Proof of ownership/ control of the telecommunication system; ▪ Proof that the interception was unauthorised; ▪ Proof that the suspect is linked to the unauthorised interception; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	It is immaterial that the unauthorised interception is not directed at a telecommunication system; any particular computer system data; a program or data of any kind; or a program or data held in any particular computer system or any of its intended effect is permanent or temporary.

3.4.2 Unauthorised Interception Resulting in Significant Financial Loss

Section	**Section 17 (2) (a)**
Description	A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system which results in significant financial loss commits an offence and is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data ▪ Causing transmission of data to or from a computer system over a telecommunication system ▪ Significant financial loss

Mens rea	▪ Intention to intercept or cause interception; and ▪ Lack of authorisation
Evidence	▪ Proof of existence of a telecommunication system; ▪ Proof of existence of a computer system; ▪ Proof of intention to intercept data from a computer system over a telecommunication system without authority; ▪ Proof of monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Proof of conduct causing transmission of data to or from a computer system over a telecommunication system; ▪ Proof of ownership/ control of the computer system from which unauthorised interception occurs; ▪ Proof of ownership/ control of the telecommunication system; ▪ Proof that the interception was unauthorized; ▪ Proof of significant financial loss resulting from the unauthorized interception; ▪ Proof that the suspect is linked to the unauthorised interception; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, NACOSTI, Judiciary, CA, ODPC, FRC, ARA, MNOs, CBK, CMA, VASPs, ISPs, Financial institutions or any other relevant agency.
General remarks	• The investigation file should clearly demonstrate the nexus between the interception and the significant financial loss. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.4.3 Unauthorised Interception which Threatens National Security
3.4.4 Unauthorised Interception which Causes Physical or Psychological Injury or Death to any Person

Section	Section 17 (2) (c)
Description	A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system which causes physical or psychological injury or death to any person commits an offence and is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

Actus reus	▪ Monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Causing transmission of data to or from a computer system over a telecommunication system; and ▪ Physical or psychological injury or death to any person
Mens rea	▪ Intention to intercept or cause interception; and ▪ Lack of authorisation
Evidence	▪ Proof of existence of a telecommunication system; ▪ Proof of existence of a computer system; ▪ Proof of intention to intercept data from a computer system over a telecommunication system without authority; ▪ Proof of monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Proof of conduct causing transmission of data to or from a computer system over a telecommunication system; ▪ Proof of ownership/ control of the computer system from which unauthorized interception occurs; ▪ Proof of ownership/ control of the telecommunication system; ▪ Proof that the interception was unauthorized; ▪ Proof of physical or psychological injury or death resulting from the unauthorized interception; ▪ Proof that the suspect is linked to the unauthorised interception; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence.
Relevant agency	NC4, NPS, MoH, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	• The investigation file should clearly demonstrate the nexus between the interception and the resultant physical/ psychological injury or death of the person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.4.5 Unauthorized Interception which Threatens Public Health or Safety

Section	Section 17 (2) (d)
Description	A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system which threatens public health or safety commits an offence and is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Causing transmission of data to or from a computer system over a telecommunication system; or ▪ Threat to public health or safety
Mens rea	▪ Intention to intercept or cause interception; and ▪ Lack of authorisation
Evidence	▪ Proof of existence of a telecommunication system; ▪ Proof of existence of a computer system; ▪ Proof of intention to intercept data from a computer system over a telecommunication system without authority; ▪ Proof of monitoring, modifying, viewing, listening to, acquiring or recording of non-public transmissions of data; ▪ Proof of conduct causing transmission of data to or from a computer system over a telecommunication system; ▪ Proof of ownership/ control of the computer system from which unauthorized interception occurs; ▪ Proof of ownership/ control of the telecommunication system; ▪ Proof that the interception was unauthorized; ▪ Proof of credible threat to public health or safety resulting from the unauthorized interception; ▪ Proof that the suspect is linked to the unauthorised interception; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, MoH, MoD, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	The investigation file should clearly demonstrate the nexus between the interception and the resultant threat to public safety

3.5 Offences Relating to Illegal Devices and Access Codes

3.5.1 Manufacture/ Sale/ Adaptation/ Procurement For Use/ Importation/ Offering to Supply/Distribution or Making Available Illegal Devices and Access Codes

Section	Section 18 (1)
Description	A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	Manufacturing/ adapting/ selling/ procuring for use/ importing/ offering to supply/ distribution or availing a device, program, computer password, access codeor similar data designed or primarily adapted to commit an offence
Mens rea	▪ Knowledge or reason to know the fact of manufacture/ sale/ adaptation/ procurement for use/ importation/ distribution or availing devices, programs, computer password, access codes or similar data
Evidence	▪ Proof of manufacture/ sale/ adaptation/ procurement for use/ importation/ distribution or availing of devices, programs, computer password access codes or similar data; ▪ Proof that the device, program, computer password or access codes are designed or primarily adapted to commit an offence; ▪ Proof of knowingly manufacturing/ adapting/ selling/ procuring for use/ importing/ offering to supply/ distribution or availing a device/ program, computer password/ access code or similar data designed or primarily adapted to commit an offence; ▪ Proof that the suspect is linked to the manufacture/ sale/ adaptation/ procurement for use/ importation/ distribution or availing of devices, programs, computer password access codes or similar data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, NACOSTI, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs, KRA or any other relevant agency.
General remarks	No offence is committed if any of the activities is intended for the authorised training, testing or protection of a computer system; or the use of a program or a computer password, access code, or similar data is undertaken in compliance of and in accordance with the terms of a judicial order issued.

3.5.2 Receipt/ Possession of Illegal Devices and Access Codes

Section	Section 18 (2)
Description	A person who knowingly receives, or is in possession of, a program or a computer password, device, access code, or similar data from any action specified under subsection (1) and intends that it be used to commit or assist in commission of an offence under this Part commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	Receipt or possession of access codes, devices or program
Mens rea	▪ Knowledge that the program, computer password, device, access code, or similar data was designed or primarily adapted for purpose of committing an offence; and ▪ Intention to use the computer password, device, access code , program or similar data to commit an offence
Evidence	▪ Proof of receipt/ possession of program, computer password, device, access code, or data designed or primarily adapted for purpose of committing an offence; ▪ Proof of intention to use the program, computer password, device, access code, or similar data to commit an offence; ▪ Proof of knowledge that the program, computer password, device, access code, or data was designed or primarily adapted for the purpose of committing an offence; ▪ Proof that the suspect is linked to the receipt/ possession of program, computer password, device, access code, or data designed or primarily adapted for purpose of committing an offence; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, NACOSTI, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	No offence is committed if any of the activities is intended for the authorised training, testing or protection of a computer system; or the use of a program or a computer password, access code, or similar data is undertaken in compliance of and in accordance with the terms of a judicial order issued.

3.6 Offences Relating to Unauthorised Disclosure of Passwords or Access Codes

3.6.1 Unauthorised Disclosure of Password or Access Code

Section	Section 19 (1)
Description	A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Disclosure of password, access code or means of gaining access to any program or data held in any computer system
Mens rea	▪ Knowledge of disclosure of the password, access code or means of gaining access to any program or data held in any computer system; and ▪ Lack of authority
Evidence	▪ Proof of existence of a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof of disclosure of password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that such disclosure of password or access code is unauthorized; ▪ Proof that the suspect is linked to the unauthorized disclosure of passwords or access codes; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	Always check if the file establishes the motivation behind the disclosure. Whether such disclosure was for any wrongful gain; for any unlawful purpose; or to occasion any loss.

3.6.2 Unauthorised Disclosure of Password or Access Code for Wrongful Gain

Section	Section 19 (2) (a)
Description	A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system for wrongful gain commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	▪ Disclosure of password, access code or means of gaining access to any program or data held in any computer system; and ▪ Wrongful gain

Mens rea	▪ Knowledge of disclosure of the password, access code or means of gaining access to any program or data held in any computer system; and ▪ Lack of authority
Evidence	▪ Proof of existence of a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof of disclosure of password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that such disclosure of password or access code is unauthorised; ▪ Proof of wrongful gain resulting from the unauthorized disclosure of password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that the suspect is linked to the unauthorized disclosure of passwords or access codes; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	• Ensure the investigation file demonstrates the nexus between the unauthorized disclosure of the password or access code and the wrongful gain. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.6.3 Unauthorised Disclosure of Password or Access Code for Unlawful Purpose

Section	Section 19 (2) (b)
Description	A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system for any unlawful purpose commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	▪ Disclosure of password, access code or means of gaining access to any program or data held in any computer system; or ▪ Unlawful purpose

Mens rea	▪ Knowledge of disclosure of the password, access code or means of gaining access to any program or data held in any computer system; or ▪ Lack of authority
Evidence	▪ Proof of existence of a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof of disclosure of password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that such disclosure of password or access code is unauthorized; ▪ Proof of an unlawful purpose resulting from the unauthorized disclosure of a password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that the suspect is linked to the unauthorized disclosure of passwords or access codes; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	• Ensure the investigation file demonstrates the nexus between the unauthorized disclosure of the password or access code and the unlawful purpose. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.6.4 Unauthorised Disclosure of Password or Access Code to Occasion a Loss

Section	Section 19 (2) (c)
Description	A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system to occasion any loss commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	▪ Disclosure of password, access code or means of gaining access to any program or data held in any computer system; and
Mens rea	▪ Knowledge of disclosure password, access code or means of gaining access to any program or data held in any computer system; ▪ Lack of authority; ▪ Intention to occasion a loss

Evidence	▪ Proof of existence of a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof of disclosure of password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that such disclosure of password or access code is unauthorized; ▪ Proof of loss resulting from the unauthorized disclosure of a password, access code or means of gaining access to any program or data held in any computer system; ▪ Proof that the suspect is linked to the unauthorized disclosure of passwords or access codes; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, ODPC, MNOs, CBK, CMA, VASPs, ISPs or any other relevant agency.
General remarks	• Ensure the investigation file demonstrates the nexus between the unauthorized disclosure of the password or access code and the intention to occasion a loss. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.7 Offences Relating to Cyber Espionage

3.7.1 Cyber Espionage in Order to Gain Unauthorized Access

Section	Section 21 (1) (a)
Description	A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to gain access, as provided under section 14, to critical data, a critical database or a national critical information infrastructure with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya commits an offence and is liable, on conviction, to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both
Actus reus	▪ Performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; and ▪ Gaining unauthorized access to critical data, critical database, national critical information infrastructure.
Mens rea	▪ Unlawful and intentional performance of the unauthorized act or unlawful and intentional authorization to a third party to perform a prohibited act; and ▪ Intention to directly or indirectly benefit a foreign state against Kenya

Evidence	▪ Proof of unauthorized access to critical data, critical database or national critical information infrastructure; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya; ▪ Proof of performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Proof that the suspect is linked to the cyber espionage; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data' ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNO's, VASPs, WPA or any other relevant agency.
General remarks	Cyber espionage investigations often involve classified intelligence or proprietary corporate secrets that victims are hesitant to reveal in open court. It is useful to consider witness protection measures from the outset.

3.7.2 Cyber Espionage in Order to Intercept Data

Section	**Section 21 (1) (b)**
Description	A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to intercept data, as provided under section 17, to, from or within a critical database or a national critical information infrastructure, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable, on conviction, to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.
Actus reus	▪ Performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; and ▪ Unauthorized interception of data, critical database, national Critical Information Infrastructure.
Mens rea	▪ Unlawful and intentional performance of the unauthorized act or unlawful and intentional authorization to a third party to perform a prohibited act; ▪ Intention to directly or indirectly benefit a foreign state against Kenya.
Evidence	▪ Proof of unauthorized interception of data from a critical database or Critical Information Infrastructure; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya; ▪ Proof of performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Proof that the suspect is linked to performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Proof of lawful acquisition of evidence e.g. Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data;

	▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNOs, VASPs, WPA or any other relevant agency.
General remarks	The investigation file should demonstrate that the espionage was for purposes of intercepting data from a critical database or national critical infrastructure.

3.7.3 Cyber Espionage Resulting in Physical Injury

Section	**Section 21 (2)**
Description	A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to gain access, as provided under section 14, to critical data, a critical database or a national critical information infrastructure with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya which results in physical injury commits an offence and is liable, on conviction, to imprisonment for a period not exceeding twenty years.
Actus reus	▪ Performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Unauthorized interception of data, critical database, national Critical Information Infrastructure; or ▪ Physical injury
Mens rea	▪ Unlawful and intentional performance of the unauthorized act or unlawful and intentional authorization to a third party to perform a prohibited act; and ▪ Intention to directly or indirectly benefit a foreign state against Kenya.
Evidence	▪ Proof of unauthorized access to/ interception of critical data, critical database or Critical Information Infrastructure; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya; ▪ Proof of performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Proof of physical injury resulting from the cyber espionage;
	▪ Proof that the suspect is linked to the unauthorized access to/ interception of critical data, critical database or Critical Information Infrastructure; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNO's, VASPs, WPA, MOH or any other relevant agency.
General remarks	The resulting physical injury should be linked to the cyber espionage.

3.7.4 Cyber Espionage Resulting in Death

Section	Section 21 (3)
Description	A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to gain access, as provided under section 14, to critical data, a critical database or a national critical information infrastructure with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya resulting in death commits an offence and is liable, on conviction, to imprisonment for life.
Actus reus	▪ Performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Unauthorized interception of data, critical database, national Critical Information Infrastructure; and ▪ Death of a person.
Mens rea	▪ Unlawful and intentional performance of the unauthorized act or unlawful and intentional authorization to a third party to perform a prohibited act; and ▪ Intention to directly or indirectly benefit a foreign state against Kenya
	▪ Proof of unauthorized access to/ interception of critical data, critical database or Critical Information Infrastructure; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya; ▪ Proof of performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Proof of death resulting from the cyber espionage; ▪ Proof that the suspect is linked to the cyber espionage;
Evidence	▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNO's, VASPs, WPA, MOH or any other relevant agency.
General remarks	The death should be linked to the cyber espionage.

3.7.5 Cyber Espionage

Section	Section 21 (4)
Description	A person who unlawfully and intentionally possesses/ communicates/ delivers/ makes available or receives, data, to, from or within a critical database or a national critical information infrastructure, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable on conviction to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.
Actus reus	▪ Possessing/ communicating/ delivering/ making available or receiving data to, from or within a critical database or a national critical information infrastructure
Mens rea	▪ Unlawfully and intentionally possessing/ communicating/ delivering or making available or receiving data to, from or within a critical database or a national critical information infrastructure; and ▪ Intention to directly or indirectly benefit a foreign state against Kenya
Evidence	▪ Proof of possession/ communication/ delivery / making available or receipt of data to, from or within a critical database or a national critical information infrastructure; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya ▪ Proof that such possession/ communication/ delivery / making available or receipt of data to, from or within a critical database or a national critical information infrastructure is unlawful; ▪ Proof that the suspect is linked to the cyber espionage; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNO's, CBK, CMA, VASPs, WPA or any other relevant agency.
General remarks	Cyber espionage investigations often involve classified intelligence or proprietary corporate secrets that victims are hesitant to reveal in open court. Explore witness protection measures from the outset.

3.7.6 Cyber Espionage

Section	Section 21 (5)
Description	A person who unlawfully and intentionally performs or authorizes, or allows another person to perform a prohibited act as envisaged under this Act in order to gain access, as provided under section 14, to or intercept data, as provided under section 17, which is in possession of the State and which is exempt information in accordance with the law relating to access to information, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a period not exceeding ten years, or to both
Actus reus	▪ Performance of an unauthorized/ authorizing/ allowing another person to perform a prohibited act under the Act; ▪ Unauthorized interception of data, critical database, national Critical Information Infrastructure; and ▪ Benefit to a foreign state against Kenya.
Mens rea	▪ Unlawful and intentional performance of the unauthorized act or unlawful and intentional authorization to a third party to perform a prohibited act; ▪ Intention to directly or indirectly benefit a foreign state against Kenya.
Evidence	▪ Proof of unauthorized access to data in a computer system which is in possession of the State and which is exempt information under the Access to Information Act, Cap 7M; ▪ Proof of unauthorized interception to data which is in possession of the State and which is exempt information under the Access to Information Act, Cap 7M; ▪ Proof of complicity by person in control of exempt information under the Access to Information Act; ▪ Proof of intention to directly or indirectly benefit a foreign state against Kenya; ▪ Proof that the suspect is linked to the cyber espionage; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	AG, MoD, MFA, NC4, NPS, Judiciary, CA, ODPC, MNO's, VASPs, CBK, CMA or any other relevant agency.
General remarks	Cyber espionage investigations often involve classified intelligence or proprietary corporate secrets that victims are hesitant to reveal in open court. Explore witness protection measures from the outset.

NB: Section 22 and 23 of the CMCA have been intentionally omitted from this Guide since the two Sections were declared unconstitutional by the Court of Appeal in Bloggers Association of Kenya (BAKE) v Attorney General & 6 others [2026] KECA 430 (KLR). However, an appeal filed at the Supreme Court is yet to be determined as at the time of the publication of this Guide (August 2026).

3.8 Offences Relating to Child Pornography

3.8.1 Publication of Child Pornography

Section	Section 24 (1) (a)
Description	A person who intentionally publishes child pornography through a computer system commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty-five years, or both.
Actus reus	Distribution/ transmission/ dissemination/ circulation/ delivery/ exhibition/ lending for gain/ exchange/ barter/ sale / offering for sale/ letting on hire /r offering to let on hire/ offering in any other way/ or making available in any way/having in possession/custody/ under control, printing/ photographing/copy or make in any other mannerchild pornography.
Mens rea	Intention to publish child pornography
Evidence	▪ Proof that the subject is a child/ looks like a child or is a synthetic depiction of a child; ▪ Proof of publication through a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof of distribution/ transmission/ dissemination/ circulation/ delivery/ exhibition/ lending for gain/exchanging/ barter/ selling or offering for sale/ letting on hire/ offering to let on hire/ offering in any other way/ or making available in any way/having in possession/custody/under control, printing/ photographing/ copying or making in any other manner child pornography; ▪ Proof that the suspect is linked to the distribution/ transmission/ dissemination/ circulation/ delivery/ exhibition/ lending for gain/exchanging/ barter/ selling or offering for sale/ letting on hire/ offering to let on hire/ offering in any other way/ or making available in any way/having in possession/custody/ under control, printing/ photographing/ copying or making in any other manner child pornography; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, DCS, ISPs, MNOs, Judiciary, CA, CBK, CMA, VASPs or any other relevant agency.
General remarks	Child pornography includes data which, whether visual or audio, depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c)realistic images representing a child engaged in sexually explicit conduct; AI-generated CSAM are covered under this section.

3.8.2 Production of Child Pornography

Section	Section 24 (1) (b)
Description	A person who intentionally produces child pornography for the purpose of its publication through a computer system commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty-five years, or both.
Actus reus	Production of child pornography
Mens rea	Intentional production of child pornography for publication through a computer system
Evidence	▪ Proof that the subject is a child/ looks like a child or is a synthetic depiction of a child; ▪ Proof of intentional production of child pornography for publication through a computer system; ▪ Proof of ownership/ control of the computer system; ▪ Proof that the suspect is linked to the intentional production of child pornography for publication through a computer system; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, DCS, ISPs, MNOs, Judiciary, CA, CBK, CMA VASPs or any other relevant agency.
General remarks	Child pornography includes data which, whether visual or audio, depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c)realistic images representing a child engaged in sexually explicit conduct; AI-generated CSAM are covered under this section.

3.8.3 Child Pornography

Section	Section 24 (1) (c)
Description	A person who intentionally downloads, distributes/ transmits/ disseminates/ circulates/ delivers/ exhibits/ lends for gain/ exchanges/ barters/ sells or offers for sale/ lets on hire or offers to let on hire/ offers in another way/ or make available in any way from a telecommunications apparatus pornography commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty-five years, or both.
Actus reus	Downloading/ distributing/ transmitting/ disseminating/ circulating/ delivering/ exhibiting/ lending for gain/ exchanging/ barter/ selling/ offering for sale/ letting on hire / offering to let on hire/ offering in any other way/ making available in any wayprinting, photographing, copying or making in any other manner pornography

Mens rea	Intention to download, distribute/ transmit/ disseminate/ circulate/ deliver/ exhibit/ lend for gain/ exchange/ barter/ sell or offer for sale/ let on hire or offer to let on hire/ offer in another way/ or make available in any way from a telecommunications apparatus pornography
Evidence	▪ Proof that the subject is a child/ looks like a child or is a synthetic depiction of a child; ▪ Proof of existence of telecommunication apparatus from which pornography is made available; ▪ Proof of ownership/ control of the telecommunication apparatus; ▪ Proof of download/, distribution/, transmission/, dissemination/, circulation/, delivery/, exhibition/, lending for gain/, exchange/, barter/, sale or offering for sale/, letting on hire or offer to let on hire/, offering in any other way/, or making available in any way/, printing/, photographing/, copying/ or making in any other manner pornography; ▪ Proof that the suspect is linked to the download/, distribution/, transmission/, dissemination/, circulation/, delivery/, exhibition/, lending for gain/, exchange/, barter/, sale or offering for sale/, letting on hire or offer to let on hire/, offering in any other way/, or making available in any way/, printing/, photographing/, copying/ or making in any other manner pornography; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, DCS, ISPs, MNOs, CA, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	Child pornography includes data which, whether visual or audio, depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c) realistic images representing a child engaged in sexually explicit conduct; AI-generated CSAM are covered under this section.

3.8.4 Possession of Child Pornography

Section	Section 24 (1) (d)
Description	A person who intentionally possesses child pornography in a computer system or on a computer data storage medium, commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty-five years, or both.
Actus reus	Existence of the child pornography in the computer system or data storage
Mens rea	Intentionally possessing
	▪ Proof that the subject is a child/ looks like a child or is a synthetic depiction of a child; ▪ Proof of possession of child pornography in a computer system or data storage medium;

Evidence	▪ Proof of ownership/ control of the computer system or data storage medium; ▪ Proof that the suspect is linked to the possession of child pornography in a computer system or data storage medium; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	DCI, DCS, NC4, ISPs, MNOs, CA, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	Child pornography includes data which, whether visual or audio, depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c) realistic images representing a child engaged in sexually explicit conduct; AI-generated CSAM are covered under this section.

3.9 Offences Relating to Computer Forgery

3.9.1 Computer Forgery

Section	Section 25 (1)
Description	A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.
Actus reus	Inputting/ altering/, deleting, or suppressing computer data resulting in inauthentic data.
Mens rea	▪ Intention to input/ alter/ delete or suppress computer data; and ▪ Intention that the data be considered or acted upon for legal purposes as if it were authentic.
Evidence	▪ Proof of inauthentic data; ▪ Proof of input/ alterations/ deletion, or suppression computer data; ▪ Proof of original computer data; ▪ Proof of intention that the data be considered or acted upon for legal purposes as if it were authentic; ▪ Proof of ownership/ control of the original computer data; ▪ Proof that the suspect is linked to the intentional input/ alterations/ deletion, or suppression computer data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.

Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	The investigation file should establish a seamless link between the altered electronic record, the specific user account responsible for the modification, and the subsequent deceptive benefit sought by the perpetrator.

3.9.2 Computer Forgery for Wrongful Gain

Section	**Section 25 (2) (a)**
Description	A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for wrongful gain commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	Inputting, altering, deleting, or suppressing computer data for wrongful gain
Mens rea	▪ Intention to input/ alter/ delete or suppress computer data; ▪ Intention that the data be considered or acted upon for legal purposes as if it were authentic; and ▪ Intent for wrongful gain
Evidence	▪ Proof of inauthentic data; ▪ Proof of input, alterations, deletion, or suppression computer data; ▪ Proof of original computer data; ▪ Proof of intent to wrongfully gain; ▪ Proof of intention that the data be considered or acted upon for legal purposes as if it were authentic; ▪ Proof of ownership/ control of the original computer data; ▪ Proof that the suspect is linked to the intentional input/ alterations/ deletion, or suppression computer data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act;
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• Demonstrate the nexus between the wrongful gain and the computer forgery. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.9.3 Computer Forgery for Wrongful Loss to Another Person

Section	Section 25 (2) (b)
Description	A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for wrongful loss to another person commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both
Actus reus	Inputting/ altering/, deleting, or suppressing computer data for wrongful loss to another person
Mens rea	▪ Intention to input/ alter/ delete or suppress computer data; ▪ Intention that the data be considered or acted upon for legal purposes as if it were authentic; and ▪ Intent for wrongful loss to another person
Evidence	▪ Proof of inauthentic data; ▪ Proof of input, alterations, deletion, or suppression computer data; ▪ Proof of original computer data; ▪ Proof of intent to cause wrongful loss to another person; ▪ Proof of intention that the data be considered or acted upon for legal purposes as if it were authentic; ▪ Proof of ownership/ control of the original computer data; ▪ Proof that the suspect is linked to the intentional input/ alterations/ deletion, or suppression computer data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, CA, ISPs, MNOs, Judiciary, CBK, CMA VASPs or any other relevant agency.
Statement of offence	• Demonstrate the nexus between the wrongful loss to another person and the computer forgery. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.9.4 Computer Forgery for an Economic Benefit for Oneself or for Another Person

Section	Section 25 (2) (c)
Description	A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for any economic benefit for oneself or for another person, commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

Actus reus	Inputting/ altering/ deleting or suppressing computer data for any economic benefit for oneself or for another person,
Mens rea	▪ Intention to input/ alter/ delete or suppress computer data; ▪ Intention that the data be considered or acted upon for legal purposes as if it were authentic; and ▪ Intent for for any economic benefit for oneself or for another person.
Evidence	▪ Proof of inauthentic data; ▪ Proof of input, alterations, deletion, or suppression computer data; ▪ Proof of original computer data; ▪ Proof of intention to have economic benefit for oneself or for another person; ▪ Proof of intention that the data be considered or acted upon for legal purposes as if it were authentic; ▪ Proof of ownership/ control of the computer data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CMA, CBK, ARA, VASPs or any other relevant agency.
General remarks	• Demonstrate the nexus between the economic benefit and the computer forgery. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10 Offences Relating to Computer Fraud

3.10.1 Computer Fraud Resulting in Unlawful Gain through an Unauthorised Access

Section	**Section 26 (1) (a) as read with 26 (2) (a)**
Description	A person who, with fraudulent or dishonest intent unlawfully gains through an unauthorised access to a computer system, program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	An unauthorised access to a computer system, program or data
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful gain resulting from the computer fraud; ▪ Proof of an unauthorised access to a computer system, program or data; ▪ Proof of fraudulent or dishonest intent ▪ Proof of ownership/ control of the computer system, program or data;

	▪ Proof that the suspect is linked to the unauthorised access to a computer system, program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of an unlawful gain. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.2 Computer Fraud Resulting in an Unlawful Gain through an Input, Alteration, Modification, Deletion, Suppression or Generation of a Program or Data

Section	**Section 26 (1) (a) as read with 26 (2) (b)**
Description	A person who, with fraudulent or dishonest intent unlawfully gains through any input, alteration, modification, deletion, suppression or generation of any program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	Any input/ alteration/ modification/deletion/ suppression or generation of any program or data;
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful gain; ▪ Proof of any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the program or data; ▪ Proof that the suspect is linked to any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the purpose of an unlawful gain.

3.10.3 Computer Fraud Resulting in Unlawful Gain through an Interference, Hindrance, Impairment or Obstruction with the Functioning of a Computer System

Section	Section 26 (1) (a) as read with 26 (2) (c)
Description	A person who, with fraudulent or dishonest intent unlawfully gains through any interference, hindrance, impairment or obstruction with the functioning of a computer system commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	Any interference/ hindrance/ impairment or obstruction with the functioning of a computer system;
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful gain; ▪ Proof of interference, hindrance, impairment or obstruction with the functioning of a computer system; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system; ▪ Proof that the suspect is linked to the interference, hindrance, impairment or obstruction with the functioning of a computer system; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of an unlawful gain. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.4 Computer Fraud Resulting in Unlawful Gain through Copying, Transferring or Moving of Data or Program to a Computer System, Data or Computer Data Storage Medium

Section	Section 26 (1) (a) as read with 26 (2) (d)
Description	A person who, with fraudulent or dishonest intent unlawfully gains through copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both

Actus reus	Copying/, transferring or moving any data or program to any computer system/, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful gain; ▪ Proof of copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program, data or computer data storage medium; ▪ Proof that the suspect is linked to the copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of an unlawful gain. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.5 Computer Fraud Resulting in Unlawful Gain through Use of Data or Program, or Possession of Data or Program Output from the Computer System in which it is Held

Section	**Section 26 (1) (a) as read with 26 (2) (e)**
Description	A person who, with fraudulent or dishonest intent unlawfully gains through use of any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both

Actus reus	Use of any data or program or possession of any data or program output from the computer system in which it is held, by having it displayed in any manner
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful gain; ▪ Proof of use of any data or program, or possession of any data or program output from the computer system in which it is held, by having it displayed in any manner; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the use of any data or program, or possession of any data or program output from the computer system in which it is held, by having it displayed in any manner; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA VASPs or any other relevant agency.
General remarks	▪ The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of an unlawful gain. ▪ Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.6 Computer Fraud Occasioning Unlawful Loss to Another Person Through an Unauthorised Access to a Computer System, Program or Data

Section	**Section 26 (1) (b) as read with 26 (2) (a)**
Description	A person who, with fraudulent or dishonest intent occasions unlawful loss to another person through an unauthorised access to a computer system, program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ An unauthorised access to a computer system, program or data ▪ Unlawful loss to another person
Mens rea	Fraudulent or dishonest intent

Evidence	▪ Proof of unlawful loss to another person; ▪ Proof of an unauthorised access to a computer system, program or data; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked unauthorised access to a computer system, program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process that occasioned unlawful loss to another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.7 Computer Fraud Occasioning Unlawful Loss to Another Person Through any Input, Alteration, Modification, Deletion, Suppression or Generation of Any Program or Data

Section	**Section 26 (1) (b) as read with 26 (2) (b)**
Description	A person who, with fraudulent or dishonest intent occasions unlawful loss to another person through any input, alteration, modification, deletion, suppression or generation of any program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Unlawful loss to another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful loss to another person ▪ Proof of any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/control of the program or data;

	▪ Proof that the suspect is linked to any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process that occasioned unlawful loss to another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.8 Computer Fraud Occasioning Unlawful Loss to Another Person Through any Interference, Hindrance, Impairment or Obstruction with the Functioning of a Computer System

Section	**Section 26 (1) (b) as read with 26 (2) (c)**
Description	A person who, with fraudulent or dishonest intent occasions unlawful loss to another person through any interference, hindrance, impairment or obstruction with the functioning of a computer system commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Any interference/, hindrance/, impairment or obstruction with the functioning of a computer system; and ▪ Unlawful loss to another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful loss to another person; ▪ Proof of interference, hindrance, impairment or obstruction with the functioning of a computer system; ▪ Proof of fraudulent or dishonest intent ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the interference, hindrance, impairment or obstruction with the functioning of the computer system; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.

Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process that occasioned unlawful loss to another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.9 Computer Fraud Occasioning Unlawful Loss to Another Person Through Copying, Transferring or Moving Data or Program to a Computer System, Data or Computer Data Storage Medium

Section	**Section 26 (1) (b) as read with 26 (2) (d)**
Description	A person who, with fraudulent or dishonest intent occasions unlawful loss to another person through copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Copying/, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; and ▪ Unlawful loss to another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful loss to another person ▪ Proof of copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.

General remarks	▪ The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process that occasioned unlawful loss to another person. ▪ Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.10 Computer Fraud Occasioning Unlawful Loss to Another Person Through Use of any Data or Program, Or Has Any Data or Program Output from the Computer System in Which It Is Held

Section	Section 26 (1) (b) as read with 26 (2) (e)
Description	A person who, with fraudulent or dishonest intent occasions unlawful loss to another person through use of any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Use of any data or program or possession of any data or program output from the computer system in which it is held, by having it displayed in any manner; or ▪ Unlawful loss to another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of unlawful loss to another person; ▪ Proof of use of any data or program, or possession any data or program output from the computer system in which it is held, by having it displayed in any manner; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the use of any data or program, or possession any data or program output from the computer system in which it is held, by having it displayed in any manner; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process that occasioned unlawful loss to another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.11 Computer Fraud Resulting in Obtaining an Economic Benefit for Oneself or for Another Person through an Unauthorised Access to a Computer System, Program or Data

Section	Section 26 (1) (c) as read with 26 (2) (a)
Description	A person who, with fraudulent or dishonest intent obtains an economic benefit for oneself or for another person through an unauthorised access to a computer system, program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ An unauthorised access to a computer system, program or data; and ▪ Obtaining an economic benefit for oneself or for another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of obtaining an economic benefit for oneself or for another person; ▪ Proof of an unauthorised access to a computer system, program or data; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the unauthorised access to a computer system, program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of routing a fraudulent economic benefit to themselves or another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.12 Computer Fraud Resulting in Obtaining an Economic Benefit for Oneself or for Another Person through any Input, Alteration, Modification, Deletion, Suppression or Generation of a Program or Data

Section	Section 26 (1) (c) as read with 26 (2) (b)
Description	A person who, with fraudulent or dishonest intent obtains an economic benefit for oneself or for another person through any input, alteration, modification, deletion, suppression or generation of any program or data commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Any input/, alteration/, modification/, deletion/, suppression or generation of any program or data; and ▪ Obtaining an economic benefit for oneself or for another person

Mens rea	▪ Fraudulent or dishonest intent
Evidence	▪ Proof of obtaining an economic benefit for oneself or for another person; ▪ Proof of any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the program or data; ▪ Proof that the suspect is linked to any input, alteration, modification, deletion, suppression or generation of any program or data; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, CA, ISPs, MNOs, Judiciary, CBK, CMA VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of routing a fraudulent economic benefit to themselves or another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.13 Computer Fraud Resulting in an Economic Benefit for Oneself or for Another Person through any Interference, Hindrance, Impairment or Obstruction with the Functioning of a Computer System

Section	**Section 26 (1) (c) as read with 26 (2) (c)**
Description	A person who, with fraudulent or dishonest intent obtains an economic benefit for oneself or for another person through any interference, hindrance, impairment or obstruction with the functioning of a computer system commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Any interference, hindrance, impairment or obstruction with the functioning of a computer system; and ▪ Obtaining an economic benefit for oneself or for another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of obtaining an economic benefit for oneself or for another person; ▪ Proof of interference, hindrance, impairment or obstruction with the functioning of a computer system; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data;

	▪ Proof that the suspect is linked to the interference, hindrance, impairment or obstruction with the functioning of a computer system; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of routing a fraudulent economic benefit to themselves or another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.14 Computer Fraud Resulting in Obtaining an Economic Benefit for Oneself or for Another Person Through Copying, Transferring or Moving any Data or Program to any Computer System, Data or Computer Data Storage Medium

Section	Section 26 (1) (c) as read with 26 (2) (d)
Description	A person who, with fraudulent or dishonest intent obtains an economic benefit for oneself or for another person through copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, prograWm, data or computer data storage medium in which it is held; commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; and ▪ Obtaining an economic benefit for oneself or for another person
Mens rea	Fraudulent or dishonest intent
Evidence	▪ Proof of obtaining an economic benefit for oneself or for another person; ▪ Proof of copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data;

	▪ Proof that the suspect is linked to the copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; ▪ Proof of lawful acquisition of evidence e.g. Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, ISPs, MNOs, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of routing a fraudulent economic benefit to themselves or another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.10.15 Computer Fraud Resulting in Obtaining an Economic Benefit for Oneself or for Another Person Through Use of Any Data or Program, or has any Data or Program Output from the Computer System in Which it is Held

Section	Section 26 (1) (c) as read with 26 (2) (e)
Description	A person who, with fraudulent or dishonest intent obtains an economic benefit for oneself or for another person through use of any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both
Actus reus	▪ Use of any data or program or has any data or program output from the computer system in which it is held, by having it displayed in any manner; and ▪ Obtaining an economic benefit for oneself or for another person
Mens rea	Fraudulent or dishonest intent
	▪ Proof of obtaining an economic benefit for oneself or for another person; ▪ Proof of use of any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner; ▪ Proof of fraudulent or dishonest intent; ▪ Proof of ownership/ control of the computer system, program or data; ▪ Proof that the suspect is linked to the use of any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner;

Evidence	▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, CA, ISPs, MNOs, JudiciaryCBK, CMA, VASPs or any other relevant agency.
General remarks	• The evidence should demonstrate a clear, uninterrupted chain showing that the suspect intentionally input false data or manipulated a system process for the express purpose of routing a fraudulent economic benefit to themselves or another person. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.11 Offences Relating to Cyber Harassment

NB: In 2025, an amendment was introduced to Section 27 (1) (b) of the CMCA to expand the scope of Cyber harassment that detrimentally affects to include communication that is likely to cause a person to commit suicide. However, the High Court in Law Society of Kenya & 8 others v Attorney General & 17 others [2026] KEHC 9453 (KLR), declared the said amendment unconstitutional. Nevertheless, this declaration of unconstitutionality was only applicable to the statement,"... or is likely to cause that other person to commit suicide" and does not affect conduct involving communication that detrimentally affects a person.

3.11.1 Cyber Harassment using Communication which is Likely to Cause Apprehension or Fear of Violence

Section	**Section 27 (1) (a) as read with Section 27 (2)**
Description	A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person commits an offence, if they know or ought to know that their conduct is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both
Actus reus	Communication that is likely to cause apprehension or fear of violence or damage or loss on that person's property
Mens rea	▪ Willfully communicating; and ▪ Knowledge that the communication is likely to cause apprehension or fear of violence or damage or loss on that person's property
Evidence	▪ Proof of communication; ▪ A transcript of the communication; ▪ Translation of the communication to English or Kiswahili; ▪ Certificate of Translation; ▪ Proof of knowledge that the communication is likely to cause apprehension or fear of violence or damage or loss on that person's property;

	▪ Proof of apprehension or fear of violence or damage or loss on that person's property; ▪ Proof that the suspect is linked to the conduct causing harassment; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, ISPs, MNOs, DCS, CA, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	A prosecutor should consider applying to court, where necessary, for an order compelling a person charged with this offence to refrain from (a) engaging or attempting to engage in; or (b) enlisting the help of another person to engage in, any harassing communication during the pendency of the trial.

3.11.2 Cyber Harassment Using Communication Which Detrimentally Affects

Section	Section 27 (1) (b) as read with Section 27 (2)
Description	A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person commits an offence, if they know or ought to know that their conduct detrimentally affects that person commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both
Actus reus	▪ Communication that is likely to detrimentally affect that person.
Mens rea	▪ Willfully communicating; and ▪ Knowledge that the communication is likely to detrimentally affect that person
Evidence	▪ Proof of communication; ▪ A transcript of the communication; ▪ Translation of the communication to English or Kiswahili; ▪ Certificate of translation; ▪ Proof of knowledge that the communication is likely to detrimentally affect that person; ▪ Proof that the person has been detrimentally affected by the communication; ▪ Proof that the suspect is linked to the conduct causing harassment; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.

Relevant agency	NC4, ISPs, MNOs, DCS, CA, NPS, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	A prosecutor should consider applying to court, where necessary, for an order compelling a person charged with this offence to refrain from (a) engaging or attempting to engage in; or (b) enlisting the help of another person to engage in, any harassing communication during the pendency of the trial.

3.11.3 Cyber Harassment using Communication of an Indecent or Gross Nature

Section	Section 27 (1) (c) as read with Section 27 (2)
Description	A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person commits an offence, if they know or ought to know that their conduct is in whole or part, of an indecent or grossly offensive nature and affects the person commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	Communication that is likely in whole or part, of an indecent or grossly offensive nature and affects the person.
Mens rea	▪ Willfully communicating; and ▪ Knowledge that the communication is likely in whole or part, of an indecent or grossly offensive nature and affects the person.
Evidence	▪ Proof that the communication is indecent or grossly offensive; ▪ Proof of knowledge that the communication is likely in whole or part, of an indecent or grossly offensive nature and affects the person; ▪ Proof that the suspect is linked to the conduct causing harassment; ▪ Translation of the communication to English or Kiswahili; ▪ Certificate of translation; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, DCS, ISPs, MNOs, CA, NPS, Judiciary, CBK, CMA, VASPs or any other relevant agency.
General remarks	A prosecutor should consider applying to court, where necessary, for an order compelling a person charged with this offence to refrain from (a) engaging or attempting to engage in; or (b) enlisting the help of another person to engage in, any harassing communication during the pendency of the trial.

3.11.4 Contravention of a Cyber Harassment Protection Order

Section	27(8)
Description	A person who is the subject of a protection order made under Section 27(3) and who contravenes that order by engaging in the communication it prohibits, commits an offence.
Actus reus	▪ Engaging in the specific communication or conduct that the protection order prohibits, after being served with or otherwise having notice of the order; and ▪ Enlisting the help of another person to engage in, any communication prohibited by the order
Mens rea	Knowledge of the existence and terms of the protection order
Evidence	▪ Proof of existence of the protection order eg. certified copy of the protection order; ▪ Proof of service or knowledge of the existence of the order; ▪ Proof of the communication alleged to contravene the order; ▪ Proof that the suspect is linked to the communication allegedly contravening the protection order; ▪ Translation of the communication to English or Kiswahili; ▪ Certificate of translation; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, MNOs, CA, Social Media Platforms, Judiciary, ISPs, WPA or any other relevant agency
General remarks	A person may apply for a Protection order under this section outside court working hours.

3.12 Offences Relating to Cybersquatting
3.12.1 Cybersquatting

Section	Section 28
Description	A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.
Actus reus	Taking or making use of a name/, business name/, trademark, domain name or other word or phrase registered or in use by another person
Mens rea	▪ Intentionally taking or making use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network; and ▪ Lack of authority/ right

Evidence	▪ Proof of registration, ownership or use of the name, business name, trademark, domain name or other word or phrase; ▪ Proof of taking or making use of a name, business name, trademark, domain name or other word or phrase registered or in use by another person; ▪ Proof that the taking or making use of the name, business name, trademark, domain name or other word or phrase was unauthorised or without right; ▪ Proof of intentional taking or making use of the name, business name, trademark, domain name or other word or phrase; ▪ Translation to English or Kiswahili; ▪ Certificate of translation; ▪ Proof that the suspect is linked to the taking or making use of the name, business name, trademark, domain name or other word or phrase was unauthorised or without right; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, ISP, MNO, DCI, CA, KIPI, KeNIC, Domain Name Registrars or any other relevant agency
General remarks	▪ Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; ▪ There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; ▪ Where there is a victim who has suffered financial loss, consider making an application under Section 45 of the CMCA for compensation

3.13 Offences Relating to Identity Theft and Impersonation

3.13.1 Identity Theft and Impersonation

Section	**Section 29**
Description	A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding three years or both.
Actus reus	Making use of the electronic signature, password or any other unique identification feature of any other person
Mens rea	Fraud or dishonesty
Evidence	▪ Proof of the electronic signature, password or any other unique identification feature of the victim; ▪ Proof of the questioned electronic signature, password or any other unique identification feature; ▪ Proof of fraud or dishonesty; ▪ Proof of making use of the electronic signature, password or any other unique identification feature of any other person;

	▪ Proof that the suspect is linked to the making use of the electronic signature, password or any other unique identification feature of any other person; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act
Relevant agency	NC4, ISP, MNO, NPS, CA, NRB, Judiciary, Social Media Providers or any other relevant agency
General remarks	▪ Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; ▪ There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; ▪ Where there is a victim who has suffered any loss, consider making an application under Section 45 of the CMCA for compensation.

3.14 Offences Relating to Phishing

3.14.1 Phishing

Section	Section 30
Description	A person who creates or operates a website or sends a message or email or makes a call through a computer system with the intention to induce the user of a website or the recipient of the message or email or call to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system, commits an offence and is liable upon conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or both.
Actus reus	Creating or operating a website or sending a message or email or making a call through a computer system
Mens rea	▪ Intention to induce the disclosure of personal information for an unlawful purpose; or ▪ Intention to gain unauthorized access to a computer system,
Evidence	▪ Proof of creating or operating a website or sending a message or email or making a call through a computer system; ▪ Proof of intention to induce the disclosure of personal information for an unlawful purpose; or ▪ Proof of intention to gain unauthorized access to a computer system; ▪ Proof that the suspect is linked to the creation or operating a website or sending a message or email or making a call through a computer system; ▪ Proof of the existence of the email/call/ message or website; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.

Relevant agency	NC4 ISP, MNO, NPS, CA, Judiciary, Domain Name Registrars or any other relevant agency.
General remarks	• Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; • There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; • Where there is a victim who has suffered financial loss, consider making an application under Section 45 of the CMCA for compensation.

3.15 Offences Relating to Interception of Electronic Messages or Money Transfer

3.15.1 Interception of Electronic Messages or Money Transfers

Section	Section 31
Description	A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or to a term of imprisonment not exceeding seven years or to both.
Actus reus	Destruction, abortion of any electronic mail or processes through which money or information is being conveyed
Mens rea	Unlawfully destroying or aborting an electronic mail or processes through which money or information is being conveyed
Evidence	▪ Proof of existence of electronic mail or processes through which money or information is being conveyed; ▪ Proof of destruction/ abortion of electronic mail or processes through which money or information is being conveyed; ▪ Proof that the destruction of electronic mail or processes through which money or information is being conveyed is unlawful ▪ Proof that the suspect is linked to destruction/ abortion of electronic mail or processes through which money or information is being conveyed; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Financial institution, CBK, CMA VASPs, Mobile Network Operators, CA, ISPs or any other relevant agency.
General remarks	• Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; • There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; • Where there is a victim who has suffered any loss, consider making an application under Section 45 of the CMCA for compensation

3.15.2 Wilful Misdirection of Electronic Messages

Section	Section 32
Description	A person who willfully misdirects electronic messages commits an offence and is liable on conviction to a fine not exceeding one hundred thousand shillings or to imprisonment for a term not exceeding two years or to both.
Actus reus	Misdirecting electronic messages
Mens rea	Willfully misdirecting electronic messages
Evidence	▪ Proof of existence of electronic message; ▪ Proof of wilful misdirection of electronic messages; ▪ Proof of the identity of the initiator/ sender of the electronic message; ▪ Proof of the identity of the intended recipient of electronic message; ▪ Proof of the identity of the wrong recipient of electronic message; ▪ Proof that the suspect is linked to the willful misdirection of electronic messages; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, MNOs, VASPs, CBK, CMA or any other relevant agency.
General remarks	• Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; • There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; • Consider applying for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.16 Offences Relating to Cyber Terrorism
3.16.1 Cyber Terrorism

Section	Section 33
Description	A person who accesses or causes to be accessed a computer or computer system or network for purposes of carrying out a terrorist act, commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both.
Actus reus	▪ Access or causing access to a computer/, computer system or network

Mens rea	Intention to commit a terrorist act
Evidence	▪ Proof of access or causing access to a computer/ computer system/ network; ▪ Proof of intention to commit a terrorist act; ▪ Proof of a terrorist act, which means an act or threat of action as defined by Section 2 of the Prevention of Terrorism Act, Cap 59B; ▪ Proof that the suspect is linked to the intention to commit a terrorist act/ the terrorist act; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA, NCTC, MNOs, CBK, CMA, VASPs and any other relevant agency.
General remarks	Refer to Section 2 of the Prevention of Terrorism Act for the definition of a terrorist act.

3.17 Offences Relating to Inducement to Deliver Electronic Message

3.17.1 Inducement to Deliver Electronic Message

Section	**Section 34**
Description	A person who induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or to both.
Actus reus	Inducing a person in charge of electronic device to deliver electronic message not specifically meant for the suspect
Mens rea	Inducing to deliver electronic message not specifically meant for the suspect
Evidence	▪ Proof of inducement to deliver any electronic messages not specifically meant for the person; ▪ Proof of delivery of electronic message; ▪ Proof of the identity of the person induced; ▪ Proof of the identity of the person inducing; ▪ Proof of the link between the suspect and the inducement; ▪ Proof of control over the electronic device; ▪ Proof that the suspect is linked to the inducement to deliver any electronic messages not specifically meant for the person; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, Judiciary, CA, MNO's, CBK, CMA, VASPs or any other relevant agency.

General remarks	• Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; • There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; • Consider applying for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.18 Offences Relating to Intentionally withholding Messages Delivered Erroneously

3.18.1 Intentionally withholding Message Delivered Erroneously

Section	Section 35
Description	A person who intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by the person or delivered to the person in error and which ought to be delivered to another person, commits an offence and is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or to both.
Actus reus	Hiding or detaining any electronic mail, message, electronic payment, credit and debit card found or delivered erroneously
Mens rea	Intention to hide or detain any electronic mail, message, electronic payment, credit and debit card found or delivered erroneously
Evidence	▪ Proof of the existence of electronic mail/, message/electronic payment/ credit and debit card; ▪ Proof that the electronic mail/ message/ electronic payment/ credit and debit card was found or delivered erroneously; ▪ Proof of hiding or detaining any electronic mail/ message/electronic payment/credit and debit card found or delivered erroneously; ▪ Proof of intention to hide or detain any electronic mail, message, electronic payment, credit and debit card found or delivered erroneously; ▪ Proof that the suspect is linked to the hiding or detaining any electronic mail/ message/electronic payment/credit and debit card found or delivered erroneously; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, ISP, MNO, Financial institution, CBK, CMA Judiciary, VASPs or any other relevant agency.
General remarks	• Prosecutors should direct financial investigations and apply for forfeiture of any resultant financial benefit to the suspect pursuant to Section 44 of the CMCA; • There is need to consider additional charges under POCAMLA for recovery of proceeds of crime as this offence is a predicate offence for money laundering; • Consider applying for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.19 Offences Relating to Unlawful Destruction of Electronic Messages
3.19.1 Unlawful Destruction of Electronic Messages

Section	Section 36
Description	A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Destruction or abortion of any electronic mail or processes through which money or information is being conveyed
Mens rea	Unlawful destruction or abortion of electronic mail or processes through which money or information is being conveyed
Evidence	▪ Proof of existence of electronic mail or processes through which money or information is being conveyed; ▪ Proof of destruction or abortion of any electronic mail or processes through which money or information is being conveyed; ▪ Proof that the destruction or abortion of any electronic mail or processes through which money or information is being conveyed is unlawful; ▪ Proof that the suspect is linked to the unlawful destruction or abortion of any electronic mail or processes through which money or information is being conveyed; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, ISPs, MNO, Financial institution, CBK, CMA, Judiciary, VASPs or any other relevant agency.
General remarks	Consider applying for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.20 Offences Relating to Wrongful Distribution of Obscene or Intimate Images
3.20.1 Wrongful Distribution of Obscene or Intimate Images

Section	Section 37
Description	A person who transfers/, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Transferring/ publishing / disseminating/ making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person
Mens rea	▪ Actus reus is sufficient to prove this offence

Evidence	▪ Proof that the image is intimate/ obscene ▪ Proof that the intimate/ obscene image belongs to another person ▪ Proof of transfer, publishing/dissemination/ making a digital depiction available for distribution or downloading intimate image of another person; ▪ Proof of transferring/ publishing / disseminating/ making a digital depiction available for distribution or downloading intimate image of another person through a telecommunications network or through any other means of transferring data to a computer; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Proof that the suspect is linked to the transferring/ publishing / disseminating/ making a digital depiction available for distribution or downloading intimate image of another person through a telecommunications network or through any other means of transferring data to a computer; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, CA, ISPs, MNOs, NPS, NC4, Judiciary or any other relevant agency.
General remarks	▪ The evidence should demonstrate that the suspect weaponized private images as an instrument of coercion and intimidation. ▪ Prosecutors should ensure that the copies of the obscene/ intimate images are deleted in all available media before withdrawing such a charge under Section 204 of the CPC or any other attempt at out of court settlement.

3.21 Offences Relating to Fraudulent Use of Electronic Data

3.21.1 Fraudulent Use of Electronic Data by Altering, Erasing, Inputting or Suppressing Any Data

Section	**Section 38 (1)**
Description	A person who knowingly and without authority causes any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Altering/, erasing/, inputting or suppressing any data stored in a computer Causing any loss of property to another
Mens rea	▪ Knowingly altering/erasing/ inputting or suppressing any data stored in a computer ▪ Altering/erasing/inputting or suppressing any data stored in a computer without authority

Evidence	▪ Proof of loss of property to another resulting from the alteration, erasure, input or suppression of any data stored in a computer; ▪ Proof of knowingly altering, erasing, inputting or suppressing any data stored in a computer without authority ▪ Proof that the suspect is linked to the alteration, erasure, input or suppression of any data stored in a computer; ▪ Proof of ownership or control of the data stored in a computer; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, Judiciary or any other relevant agency.
General remarks	Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.21.2 Fraudulent Use of Electronic Data which Materially Misrepresents any Fact

Section	**Section 38 (2)**
Description	A person who sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss commits an offence and is liable on conviction to imprisonment for a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	▪ Sending an electronic message which materially misrepresents any fact; and ▪ Damage or loss
Mens rea	Misrepresentation of any fact
Evidence	▪ Proof of misrepresentation of any fact; ▪ Proof of reliance by another person on the misrepresented fact; ▪ Proof of the identity of the person who relied on the misrepresented fact; ▪ Proof of damage or loss suffered by another person; ▪ Proof of the link between the suspect and the sending of an electronic message which materially misrepresents any fact; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.21.3 Fraudulent Use of Electronic Data by Franking Electronic Messages/ Instructions or Subscribing to any Electronic Messages/ Instructions

Section	Section 38 (3)
Description	A person who, with intent to defraud, franks electronic messages, instructions, subscribes any electronic messages or instructions, commits an offence and is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Franking electronic messages or instructions/ subscribing any electronic messages or instructions
Mens rea	Intention to defraud
Evidence	▪ Proof of franking/ subscribing any electronic messagesor instructions; ▪ Proof of intention to defraud; ▪ Proof of link between the suspect and the franking/ subscribing any electronic messages or instructions; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	• The evidence should demonstrate that the data layer was intentionally weaponized, by franking electronic messages/ instructions or subscribing to any electronic messages/ instructions. • Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.21.4 Fraudulent Use of Electronic Data by Manipulating a Computer or Other Electronic Payment

Section	Section 38 (4)
Description	A person who manipulates a computer or other electronic payment device with the intent to short pay or overpay commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Manipulating a computer or electronic payment device
Mens rea	Intention to short pay or overpay
Evidence	▪ Proof of manipulation of a computer or electronic payment device; ▪ Proof of intention to short pay/overpay; ▪ Proof of the link between the suspect and the manipulation of a computer or electronic payment device; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.

Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	A person convicted under this Section shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

3.22 Offences Relating to Issuance of False e-Instructions

3.22.1 Issuance of False e-Instructions

Section	**Section 39**
Description	A person authorized to use a computer or other electronic devices for financial transactions including posting of debit and credit transactions, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or confirmation of electronic fund transfer, issues false electronic instructions, commits an offence and is liable, on conviction, a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Issuance of false electronic instructions to a computer or electronic device for financial transaction
Mens rea	Intention to falsify the e-instructions
Evidence	▪ Proof that a person has authority to use a computer or other electronic device for financial transactions; ▪ Proof of the correct electronic instructions relating to sending of electronic debit and credit messages or confirmation of electronic fund transfer; ▪ Proof of issuance of false electronic instructions relating to sending of electronic debit and credit messages or confirmation of electronic fund transfer; ▪ Proof of financial transactions; ▪ Proof of link between the suspect to the issuance of false electronic instructions relating to sending of electronic debit and credit messages or confirmation of electronic fund transfer; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, DCI, Financial institution, CBK, CMA, VASPs or any other relevant agency.
General remarks	Prosecutors should apply for a compensation order under Section 45 of the CMCA for any resultant loss to the victim, caused by the commission of the offence, upon conviction of the accused person.

3.23 Offences Relating to Failure to Report a Cyber Threat
3.23.1 Failure to Report a Cyber Threat

Section	Section 40 (4)
Description	A person who operates a computer system or a computer network, whether public or private, shall immediately inform the Committee of any attacks, intrusions and other disruptions to the functioning of another computer system or network within twenty-four hours of such attack, intrusion or disruption commits an offence and is liable upon conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Failure to report any attacks, intrusions and other disruptions to the functioning of another computer system or network within twenty-four hours of such attack, intrusion or disruption
Mens rea	The offence is complete when a person fails to report
Evidence	▪ Proof of any attacks, intrusions and other disruptions to the functioning of another computer system or network; ▪ Proof of failure to report any attacks, intrusions and other disruptions to the functioning of another computer system or networkto NC4; ▪ Proof that the person operates a computer system or a computer network, whether public or private network; ▪ Proof of lapse of 24 hrs of such attack, intrusion or disruption; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, Judiciary or any other relevant agency.
General remarks	Demonstrate noncompliance by the entity that is incurable by mere administrative action.

3.24 Offences Relating to Failure to Relinquish Access Codes upon Termination of Employment
3.24.1 Failure to Relinquish Access Codes upon Termination of Employment

Section	Section 41
Description	An employee, who, subject to any contractual agreement between the employer and the employee, fails to relinquish all codes and access rights to their employer's computer network or system immediately upon termination of employment commits an offence and shall be, liable on conviction, to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.
Actus reus	Failure to relinquish access all codes and access rights to their employer's computer network or system immediately upon termination of employment
Mens rea	Unwillingness to relinquish access rights and codes

Evidence	▪ Proof of employment; ▪ Proof of termination of employment; ▪ Proof of demand to relinquish the access codes and access rights; ▪ Proof of failure to relinquish the access codes and access rights despite demand; ▪ Proof that the access codes and access rights are within the ownership/ control of the computer network or system of the suspect's employer; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, Judiciary, CA, NC4 or any other relevant agency.
General remarks	The investigation file should demonstrate that the retention was not a mere oversight. This is best achieved by showing that the suspect ignored formal exit protocols, failed to respond to direct demands to hand over access codes, or active steps were taken to hide the fact that they still held access.

3.25 Offences Relating to Aiding or Abetting

3.25.1 Aiding or Abetting in the Commission of an Offence under the Act

Section	Section 42 (1)
Description	A person who knowingly and willfully aids or abets the commission of any offence under this Act commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.
Actus reus	Aiding or abetting the commission of an offence under the Act
Mens rea	▪ Knowledglyaiding and abetting the commission of an offence under the Act; and ▪ Willfully aiding or abetting the commission of an offence under the Act
Evidence	▪ Proof of knowingly and willfully aiding or abetting any offence under the Act; ▪ Proof of direct link between the suspect and the aiding or abeting of the offence. ▪ Proof of lawful acquisition of evidence e.g. Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act
Relevant agency	NPS, NC4, CA, Judiciary or any other relevant agency.
General remarks	The evidence should show a direct link of the assistance offered to the offence committed.

3.25.2 Attempting the Commission of an Offence Under the Act

Section	Section 42 (2)
Description	A person who knowingly and willfully attempts to commit an offence or does any act preparatory to or in furtherance of the commission of any offence under this Act, commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.
Actus reus	Attempt to commit an offence under the Act
Mens rea	▪ Knowingly attempting to commit an offence under the Act; and ▪ Willfully attempting to commit an offence under the Act
Evidence	▪ Proof of knowingly and willfully attempting to commit an offence under the Act; ▪ Proof of direct link between the suspect and the attempt to commit an offence under the Act ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	NPS, NC4, CA, Judiciary or any other relevant agency.
General remarks	The evidence should demonstrate proof that the accused took a concrete, physical step toward executing that intent. This step must go beyond mere preparation and be part of a series of actions that would have resulted in the completed crime if not interrupted.

3.26 Offences Relating to Body Corporates

3.26.1 Offences by Body Corporates

Section	Any section creating the offence as read with Section 43(1)(a) /(b)
Description	Where any offence under this Act has been committed by a body corporate: the body corporate is liable, on conviction, to a fine not exceeding fifty million shillings; and every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity, is also deemed to have committed the offence, unless they prove that the offence was committed without their consent or knowledge and that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their functions and to prevailing circumstances, and is liable, on conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both.
Actus reus	▪ As per the specific offence under the Act; and ▪ Failure to exercise such diligence to prevent the commission of the offence
Mens rea	The respective mens rea for each of the offences under the Act

Evidence	▪ Proof of commission of an offence under the Act; ▪ Proof that the offence is committed by a by a body corporate; ▪ Proof that the person is a principal officer of the body corporate, or anyone acting in a similar capacity; ▪ Proof that the principal officer of the body corporate, or anyone acting in a similar capacity failed to exercise such diligence to prevent the commission of the offence; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act.
Relevant agency	BRS, NPS, NC4, Judiciary, ISPs, MNOs, CA or any other relevant agency.
General remarks	This section does not create any new offence, instead, it has a distinct penalty when the offender is a body corporate. This should be factored when making a charging decision and at the sentencing hearing.

3.27 Offences Relating to Search and Seizure

3.27.1 Obstructing the Lawful Exercise of Powers Pursuant to a Warrant

Section	Section 48 (5) (a)
Description	A person who obstructs the lawful exercise of the powers under this section commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both.;
Actus reus	Obstructing lawful exercise of investigative powers under Section 48 of the CMCA
Mens rea	Knowledge of the exercise of investigative powers under Section 48 of the CMCA
Evidence	▪ Proof of obstruction of the lawful exercise of investigative powers under Section 48 of the CMCA; and ▪ Proof of existence of a search and seizure warrant under Section 48 of the CMCA.
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	This offence is limited to obstruction done in the course of executing a search and seizure warrant.

3.27.2 Compromising the Integrity or Confidentiality of a Computer System, Data, or Information Accessed or Retained

Section	Section 48 (5) (b)
Description	A person who compromises the integrity or confidentiality of a computer system, data, or information accessed or retained under this section commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both.;

Actus reus	Compromising the integrity or confidentiality of a computer system/, data, or information accessed or retained
Mens rea	Lack of authority
Evidence	▪ Proof of Compromising the integrity or confidentiality of a computer system/, data, or information accessed or retained without authorization; ▪ Proof of lawful acquisition of evidence eg Court orders authorising search, seizure, or exploration; or Mutual Legal Assistance (MLA) transmission orders for cross-border data; ▪ Certificate of electronic evidence pursuant to Section 106B of the Evidence Act
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	This offence is limited to compromising the integrity or confidentiality of a computer system, data, or information accessed or retained pursuant to a search and seizure warrant under Section 48 of the CMCA.

3.27.3 Misuse of Investigative Powers Pursuant to a Warrant

Section	Section 48 (5) (c)
Description	A person who misuses the powers granted under this section commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both.
Actus reus	Misusing investigative powers granted under Section 48 of the CMCA
Mens rea	Knowledge of the powers specified in the warrant
Evidence	▪ Proof of misuse of investigative powers granted under Section 48 of the CMCA; and ▪ Proof of existence of a search and seizure warrant under Section 48 of the CMCA
Relevant agency	NC4, NPS, Judiciary, CA, IPOA or any other relevant agency.
General remarks	This offence is limited to misuse of investigative powers pursuant to a search and seizure warrant granted under Section 48 of the CMCA

3.28 Offences Relating to Section 52 of the CMCA

3.28.1 Failure to Comply with a Court Order Issued Pursuant to Section 52

Section	Section 52 (7)
Description	(a) A service provider who fails to comply with an order under this section commits an offence and is liable on conviction where the service provider is a corporation, to a fine not exceeding ten million shillings (b) in case of a principal officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Failure to comply with a court order issued under Section 52 of the CMCA
Mens rea	Knowledge of the existence of the court order

Evidence	▪ Proof that the suspect is a service provider, or a principal officer of the service provider; ▪ Proof of the existence of a court order issued under Section 52 of the CMCA; ▪ Proof of service of the court order upon the service provider or principal officer of the service provider; ▪ Proof of noncompliance with the court order.
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	The evidence must demonstrate that the service provider or principal officer was served with the order.

3.29 Offences Relating to Section 53 of the CMCA

3.29.1 Failure to Comply with a Court Order Issued Pursuant to Section 53

Section	**Section 53 (7)**
Description	(a) A service provider who fails to comply with an order under this section commits an offence and is liable on conviction where the service provider is a corporation, to a fine not exceeding ten million shillings (b) in case of an officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Failing to comply with a court order on interception of content order
Mens rea	Knowledge of the existence of the court order.
Evidence	▪ Proof that the suspect is a service provider, or an officer of the service provider; ▪ Proof of existence of a court order issued pursuant to Section 53 of the CMCA; ▪ Proof of service of the court order upon the service provider or an officer of the service provider; ▪ Proof of noncompliance with the court order
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	The evidence must demonstrate that the service provider or officer was served with the order.

3.30 Offences Relating to Investigations

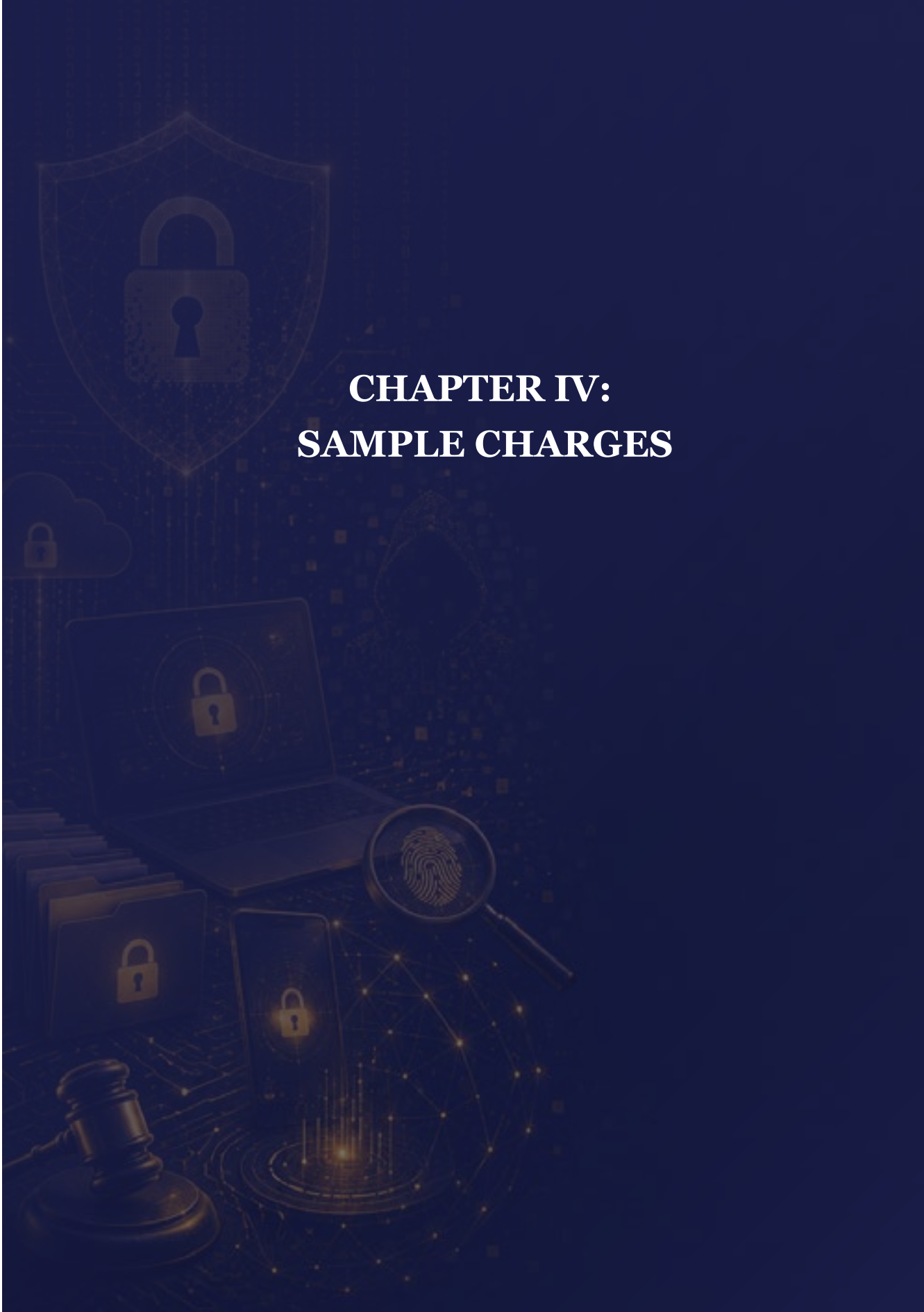
3.30.1 Obstruction of Lawful Investigations

Section	**Section 54 (1)**
Description	A person who obstructs the lawful exercise of the powers under this Part, including destruction of data, or fails to comply with the requirements of this Part is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Obstruction of lawful investigation procedures under Part IV of the CMCA
Mens rea	Knowledge of ongoing investigations

Evidence	▪ Proof of obstruction of lawful investigations under Part IV of the CMCA; and ▪ Proof of existence of warrants issued pursuant to Part IV of the CMCA
Relevant agency	NC4, NPS, Judiciary, CA or any other relevant agency.
General remarks	The evidence must demonstrate the manner in which the suspect obstructed lawful investigations.

3.30.2 Misuse of Investigative Powers

Section	**Section 54 (2)**
Description	A police officer or an authorised person who misuses the exercise of powers under this Part commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Actus reus	Misuse of powers under Part IV of the CMCA
Mens rea	Knowledge of the powers granted under Part IV of the CMCA
Evidence	▪ Proof that the person is a police officer or an authorised officer under the CMCA; ▪ Proof of misuse of investigative powers under Part IV of the CMCA; ▪ Proof of scope of investigative powers allegedly misused.
Relevant agency	NPS, NC4, Judiciary, CA or any other relevant agency.
General remarks	Knowledge of the powers granted under Part IV can be inferred by court orders granting the powers as well as the mere fact of being a police officer or an authorised person under the CMCA.



CHAPTER IV:
SAMPLE CHARGES

CHAPTER IV

SAMPLE CHARGES

This Chapter outlines the template charges for offences under the CMCA. The selection and institution of appropriate charges must strictly adhere to the provisions of Section 134 of the Criminal Procedure Code on framing of charges as well as the ODPP Decision to Charge Guidelines, 2019. Consequently, prosecutors and investigators are required to exercise due care and attention to ensure that the specific charge preferred accurately reflects the distinct facts and evidentiary nuances of the case from the various options provided. Care should be taken to ensure that all bracketed texts are replaced with specific factual details, befitting the circumstances of the case, prior to filing of the Charge Sheets.

4.1 Charges Relating to Auditing of Critical Information Infrastructure

4.1.1 FAILURE TO FILE A COMPLIANCE REPORT/FAILURE TO COOPERATE WITH AN AUDIT ON A CRITICAL INFORMATION INFRASTRUCTURE CONTRARY TO SECTION 13 (5) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....being an owner/authorized person in control of a critical information infrastructure, you failed to file a compliance report.... {(Specify the reporting period)...../failed to cooperate with an audit.....(Specify the nature of the audit/ auditing period)}.....on ..... (Specify the critical information infrastructure).....

4.1.2 FAILURE TO PROVIDE ADDITIONAL INFORMATION TO THE DIRECTOR NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE CONTRARY TO SECTION 13 (5) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (Any other)

On .....(date)..... at .....(location).....being an owner/authorized person in control of a critical information infrastructure, you failed to provide additional information to the Director, National Computer and Cybercrime Coordination Committee, to wit,.... (Specify the additional information requested).....on.....(Specify the critical information infrastructure).....

4.1.3 HINDERING, OBSTRUCTING OR ATTEMPTING TO INFLUENCE A MEMBER OF THE NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE/PERSON/ENTITY CONTRARY TO SECTION 13 (5) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....being an owner/authorized person in control of a critical information infrastructure.....(Specify the critical information infrastructure)..... you.....(hindered, obstructed or attempted to influence).....(a member of the National Computer and Cybercrimes Coordination Committee/person/entity)..... to .....(monitor, evaluate and report).....on the adequacy and effectiveness of an audit.....by .....(Specify the specific action).....

4.1.4 HINDERING, OBSTRUCTING OR ATTEMPTING TO INFLUENCE AUTHORIZED PERSON CONTRARY TO SECTION 13 (5) (d) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....being an owner/authorized person in control of a critical information infrastructure.....(Specify the critical information infrastructure)..... you.....(hindered, obstructed or attempted to influence).....(Specify the authorized person).....to carry out an audit.....(Specify an audit).....by.....(Specify the action).....

4.1.5 FAILURE TO COOPERATE WITH AUTHORIZED PERSON CONTRARY TO SECTION 13 (5) (e) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....being an owner/authorized person in control of a critical information infrastructure.....(*Specify the critical information infrastructure*)..... you.....failed to cooperate with.....*(Specify the authorized person)*.....to carry out an audit.....(*Specify an audit*).....by.....*(Specify the action)*.....

4.1.6 FAILURE TO ASSIST OR PROVIDE TECHNICAL ASSISTANCE OR SUPPORT TO AUTHORIZED PERSON CONTRARY TO SECTION 13 (5) (f) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....being an owner/authorized person in control of a critical information infrastructure.....(*Specify the critical information infrastructure*)..... you.....failed to assist/provide technical assistance and support to.....*(Specify the authorized person)*.....to carry out an audit.....(*Specify an audit*).....by.....*(Specify the action)*.....

4.2 Charges Relating to Unauthorised Access to a Computer System

4.2.1 UNAUTHORISED ACCESS TO A COMPUTER SYSTEM CONTRARY TO SECTION 14 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you infringed security measures of .....(entity)..... and without authority gained access to .....(specify the *computer system*).....

4.2.2 UNAUTHORISED ACCESS TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 14 (1) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you infringed security measures of .....(entity)..... and without authority gained access to .....(Specify the *protected computer system*).....

4.2.3 ACCESS WITH INTENT TO COMMIT FURTHER OFFENCE CONTRARY TO SECTION 15 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you infringed security measures of .....(*entity*)..... and gained access to .....(specify the *computer system*)..... and upon such access you committed a further offence namely, ...*(specify the offence)*.....

4.2.4 ACCESS TO A PROTECTED COMPUTER SYSTEM WITH INTENT TO COMMIT FURTHER OFFENCE CONTRARY TO SECTION 15 (1) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C.

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you infringed security measures of .....(specify the entity)..... and without authority gained access to ..... (Specify the *protected computer system*)..... and upon such access you committed a further offence namely, ...*(specify the further offence)*.....

4.3 Charges Relating to Interference to Computer Sytem, Data or Program

4.3.1 UNAUTHORISED INTERFERENCE CONTRARY TO SECTION 16 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority,did an act, to wit.....(*describe the specifc act causing interference*)....causing an unauthorised inteferance to .....(*computer system/data/program*).....

4.3.2 UNAUTHORISED INTERFERENCE TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 16 (1) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interference*)..... causing an unauthorised inteferance to .....(*Specify the protected computer system/data/program*).....

4.3.3 UNAUTHORISED INTERFERENCE CONTRARY TO SECTION 16 (3) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc actcausing interference*)..... causing an unauthorised inteferance to .....(*computer system/data/program*)..... which resulted in a significant financial loss).

4.3.4 UNAUTHORISED INTERFERENCE TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 16 (3) (a) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority *jointly* did an act, to wit.....(*describe the specifc act causing interference*)..... causing an unauthorised inteferance to .....(Specify the protected *computer system/data/program*)..... which resulted in a signifcant financial loss).

4.3.5 UNAUTHORISED INTERFERENCE CONTRARY TO SECTION 16 (3) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interference*)....causing an unauthorised inteferance to .....(*computer system/data/programme*)..... which threatened national security.

4.3.6 UNAUTHORISED INTERFERENCE TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 16 (3) (b) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interference*)....causing an unauthorised inteferance to .....(Specify the protected *computer system/data/program*)..... which threatened national security.

4.3.7 UNAUTHORISED INTERFERENCE CONTRARY TO SECTION 16 (3) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act).... .....causing an unauthorised inteferance to .....(computer system/data/program)..... which caused (physical injury / death) to [specify the identity of the person who suffered physical injury or death).

4.3.8 UNAUTHORISED INTERFERENCE TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 16 (3) (c) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act causing interference)..... causing an unauthorised inteferance to .....(Specify the protected computer system/data/program)..... which caused (physical injury / death) to (specify the identity of the person who suffered physical injury or death).

4.3.9 UNAUTHORISED INTERFERENCE CONTRARY TO SECTION 16 (3) (d) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act causing interference)..... .....causing an unauthorised inteferance to .....(computer system/data/program)..... which threatened (public health / public safety).

4.3.10 UNAUTHORISED INTERFERENCE TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 16 (3) (d) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act causing interference)..... .....causing an unauthorised inteferance to .....(Specify the protected computer system/data/program)..... which threatened (public health / public safety).

4.4 Charges Relating to Unauthorised Interception

4.4.1 UNAUTHORISED INTERCEPTION CONTRARY TO SECTION 17 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act causing interception)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the computer system) over a .... (specify the telecommunication system)

4.4.2 UNAUTHORISED INTERCEPTION OF A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 17 (1) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(describe the specifc act causing interception)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the protected computer system) over a .... (specify the telecommunication system)

4.4.3 UNAUTHORISED INTERCEPTION CONTRARY TO SECTION 17 (2) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the computer system) over a .... (specify the telecommunication system) which resulted in a significant financial loss).

4.4.4 UNAUTHORISED INTERCEPTION OF A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 17 (2) (a) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the protected computer system) over a .... (specify the telecommunication system)..... which resulted in a significant financial loss).

4.4.5 UNAUTHORISED INTERCEPTION CONTRARY TO SECTION 17 (2) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the computer system) over a .... (specify the telecommunication system)... which threatened national security.

4.4.6 UNAUTHORISED INTERCEPTION OF A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 17 (2) (b) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the protected computer system) over a .... (specify the telecommunication system)..... which threatened national security.

4.4.7 UNAUTHORISED INTERCEPTION CONTRARY TO SECTION 17 (2) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the computer system) over a .... (specify the telecommunication system)... which caused physical / psychological injury / death to (specify the identity of the victim of physical/ psychological injury or death)

4.4.8 UNAUTHORISED INTERCEPTION TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 17 (2) (c) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the protected computer system) over a .... (specify the telecommunication system)..... which caused (physical/ psychological injury / death) to (specify the identity of the victim of physical, psychological injury or death)

4.4.9 UNAUTHORISED INTERCEPTION CONTRARY TO SECTION 17 (2) (d) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the computer system) over a .... (specify the telecommunication system)... which threateed public health or public safety.

4.4.10 UNAUTHORISED INTERCEPTION TO A PROTECTED COMPUTER SYSTEM CONTRARY TO SECTION 17 (2) (d) AS READ WITH SECTION 20 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you intentionally and without authority did an act, to wit.....(*describe the specifc act causing interception*)..... .....which intercepted data being transmitted..... (to/ from) .....(specify the protected computer system) over a .... (specify the telecommunication system)..... which threatened public health or public safety.

4.5 Charges Relating to Illegal Devices and Access Codes

4.5.1 MANUFACTURE/ADAPTATION/SALE/PROCUREMENT FOR USE/ IMPORTATION/OFFERING TO SUPPLY/DISTRIBUTION OR MAKING AVAILABLE (SELECT ONE) ILLEGAL DEVICES AND ACCESS CODES CONTRARY TO SECTION 18 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you knowingly manufactured/adapted/sold/procured for use/imported/offered to supply/distributed or made available (select one) a devices/programme/computer password/access codes (elect one) designed or adapted to commit an offence namely .....

4.5.2 POSSESSION/ RECEIPT OF ILLEGAL DEVICES AND ACCESS CODES CONTRARY TO SECTION 18 (2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you knowingly received or were in possession/ receipt (select one) of *a* devices/programme/computer password/ access codes *(elect one)* designed or adapted to commit an offence namely .....

4.6 Charges Relating to Unauthorised Disclosure of Password or Access Codes

4.6.1 UNAUTHORISED DISCLOSURE OF PASSWORD OR ACCESS CODE CONTRARY TO SECTION 19(1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)....., within the Republic of Kenya, you knowingly and without authority disclosed passwords/access codes or .....(any other means).....to gain access to (data/programme) in a .....computer system).....

4.6.2 UNAUTHORISED DISCLOSURE OF PASSWORD OR ACCESS CODE CONTRARY TO SECTION 19 (2) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you knowingly and without authority disclosed passwords/access codes or .....*(any other means)*..... to gain access to (data/program) in a .....*computer system)*.....for .....(indicate any *wrongful gain)*.....

4.6.3 UNAUTHORISED DISCLOSURE OF PASSWORD OR ACCESS CODE CONTRARY TO SECTION 19 (2) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you knowingly and without authority disclosed passwords/access codes or .....*(any other means)*..... to gain access to (data/programme) in a .....*computer system)*.....for .....(indicate any *unlawful purpose)*.....

4.6.4 UNAUTHORISED DISCLOSURE OF PASSWORD OR ACCESS CODE CONTRARY TO SECTION 19 (2) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*....., within the Republic of Kenya, you knowingly and without authority disclosed passwords/access codes or .....*(any other means)*..... to gain access to *(data/programme)* in a .....*computer system)*.....for .....(indicate any *loss)*.....

4.7 Charges Relating to Cyber Espionage

4.7.1 CYBER ESPIONAGE CONTRARY TO SECTION 21 (1) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....you unlawfully and intentionally performed or authorized or allowed another person to perform a prohibited act namely .....in order to gain access.....*(critical database/ national critical information infrastructure)*.....to benefit a foreign state against the Republic of Kenya.

4.7.2 CYBER ESPIONAGE CONTRARY TO SECTION 21 (1) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....you unlawfully and intentionally performed or authorized or allows another person to perform a prohibited act namely .....in order to intercept data .....*(critical database/ national critical information infrastructure)*..... to benefit a foreign state against the Republic of Kenya.

4.7.3 CYBER ESPIONAGE CONTRARY TO SECTION 21 (2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....you unlawfully and intentionally performed or authorized or allows another person to perform a prohibited act namely .....in order to.....(gain access/intercept data).....to.....(critical database/national critical information infrastructure).....to benefit a foreign state against the Republic of Kenya and caused physical injury to .....(name the person).....

4.7.4 CYBER ESPIONAGE CONTRARY TO SECTION 21 (3) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....you unlawfully and intentionally performed or authorized or allows another person to perform a prohibited act namely .....in order to .....(gain access/intercept data).....to.....(critical database/ national critical information infrastructure).....to benefit a foreign state against the Republic of Kenya and led to death of .....(name the person).....

4.7.5 CYBER ESPIONAGE CONTRARY TO SECTION 21 (4) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....you unlawfully and intentionally possessed, communicated, delivered, or made available or received, data, to, from, or within .....*(critical database or national critical information infrastructure)*..... with.....(intention)..... to benefit a foreign state against the Republic of Kenya.

4.7.6 CYBER ESPIONAGE CONTRARY TO SECTION 21 (5) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location).....you unlawfully and intentionally performed or authorised, or allowed another .....(person).....to perform prohibited act in order to..... (access/intercept data)..... in possesion of the State, and which is exempt information in accordance with the law relating to access to information with the intention to directly or indirectly benefit a foreign State against the Republic of Kenya.

4.8 Charges Relating to Child Pornography

4.8.1 CHILD PORNOGRAPHY CONTRARY TO SECTION 24 (1) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally published child pornography through a .....*(Specify the computer system)*.....

4.8.2 CHILD PORNOGRAPHY CONTRARY TO SECTION 24 (1) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....(date)..... at .....(location)..... you intentionally produced child pornography for the purposes of publication through a .....(computer system).....

4.8.3 CHILD PORNOGRAPHY CONTRARY TO SECTION 24 (1) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally .....*(downloaded/ distributed/transmited/disseminated/circulated/delivered/exhibited/lended for gain/ exchanged/bartered/sold or offered for sale/hired or offered to let on hire/offered in another way/or made available in any way from a telecommunications apparatus)*.....*(choose appropriate action befitting the circumstances of the case)*.....pornography.

4.8.4 CHILD PORNOGRAPHY CONTRARY TO SECTION 24 (1) (d) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally possessed child pornography in a .....*(computer system/on a computer data storage medium)*.....

4.9 Charges Relating to Computer Forgery

4.9.1 COMPUTER FORGERY CONTRARY TO SECTION 25 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally .....*(inputed/altered/ deleted/suppressed)*..... computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible

4.9.2 COMPUTER FORGERY CONTRARY TO SECTION 25 (2) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally .....*(inputed/altered/deleted/suppressed)*..... computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for wrongful gain.

4.9.3 COMPUTER FORGERY CONTRARY TO SECTION 25 (2) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*.....you intentionally .....*(inputed/altered/deleted/suppressed)*..... computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for wrongful loss to another person.

4.9.4 COMPUTER FORGERY CONTRARY TO SECTION 25 (2) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On .....*(date)*..... at .....*(location)*..... you intentionally .....*(inputed/altered/deleted/suppressed)*..... computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible for any economic benefit for .....(*oneself/another person)*.....

4.10 Charges Relating to Computer Fraud

4.10.1 COMPUTER FRAUD CONTRARY TO SECTION 26 (1) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF THE OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....with fraudulent or dishonest intent you unlawfully gained .....*(Specify the gain)* .....by.....*(means of unauthorised access to a computer system/program/data)..... or any other means as specified under section 26 (2) of the Act*.....

4.10.2 COMPUTER FRAUD CONTRARY TO SECTION 26 (1) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....(name)..... with fraudulent or dishonest intent unlawfully occasions loss .....(Specify the loss) .....to ..... (Specify the person).....by.....(means of unauthorised access to a computer system/program/data)..... or any other means as specified under section 26 (2) of the Act.....

4.10.3 COMPUTER FRAUD CONTRARY TO SECTION 26 (1) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....(name)..... with fraudulent or dishonest intent you unlawfully obtained an economic benefit.....(Specify the economic benefit).....for.....(oneself/another person)..... (means of unauthorised access to a computer system/program/data)..... or any other means as specified under section 26 (2) of the Act.....

4.11 Charges Relating to Cyber Harassment

4.11.1 CYBER HARASSMENT CONTRARY TO SECTION 27(1) (a) AS READ WITH SECTION 27(2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....(*name)*.....
You willfully communicated, with ..... *(name the person/anyone known to that person)* .....whilst knowing or ought to have known that such communication is likely to cause ..... *(name of the said person)*.....*(apprehension/fear of violence to them/damage/loss on .....(name of that person's)*..... property.

4.11.2 CYBER HARASSMENT CONTRARY TO SECTION 27(1) (b) AS READ WITH SECTION 27(2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....(*name)*.....
You willfully communicated, with ..... *(name the pers...on/anyone known to that person)* .....whilst knowing or ought to have known that such communication will detrimentally affect.....*(name of the said person)*.....

4.11.3 CYBER HARASSMENT CONTRARY TO SECTION 27 (1) (c) AS READ WITH SECTION 27(2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....(*name)*.....
You willfully communicated, with ..... *(name the person/anyone known to that person)* .....whilst knowing or ought to have known that such communication is in .....(whole/part), of an indecent or grossly offensive nature and affects .....*(name of the said person)*.....

4.11.4 CONTRAVENTION OF A COURT ORDER CONTRARY TO SECTION 27 (8) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....(name)..... you contravened a court order compelling you to refrain from engaging/attempting to engage in.....(specify the action)/.....enlisting the help of another person to engage in any communication complained of .....(specify the communication)...../service provider failed to provide any subscriber information in its possession as per the order.....(specify the details in the order).....

4.12 Charges Relating to Cybersquatting

4.12.1 CYBERSQUATTING CONTRARY TO SECTION 28 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....(*name)*..... you intentionally .....*(took/made)*.....use of a *(name/business name/trademark/domain name/other word/phrase)*.....*(registered/owned/in use)* by.....*(give details of the person or computer network)*.....without (*authority/right)*.....

4.13 Charges Relating to Identity Theft and Impersonation

4.13.1 IDENTITY THEFT AND IMPERSONATION CONTRARY TO SECTION 29 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....(*name)*.....you fraudulently or dishonestly made use of the .....*(electronic signature/password/any other unique identification feature*) of .....*(Specify the person*) .....

4.14 Charges Relating to Phishing

4.14.1 PHISHING CONTRARY TO SECTION 30 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you.....{(created/operated a website)/ sends a message/email/made a call} through a computer system with the intention to induce .....(the user of a website/the recipient of the message/email/call)..... to disclose personal information for .....(specify the an unlawful purpose/to gain unauthorized access to a computer system).

4.15 Charges Relating to Interception of Electronic Messages or Money Transfers

4.15.1 INTERCEPTION OF ELECTRONIC MESSAGES OR MONEY TRANSFERS CONTRARY TO SECTION 31 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....you unlawfully .....*(destroyed/ aborted)*.....*(electronic mail/processes through which money or information is being conveyed)*.....

4.16 Charges Relating to Willful Misdirection of Electronic Messages

4.16.1 WILLFUL MISDIRECTION OF ELECTRONIC MESSAGES CONTRARY TO SECTION 32 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you willfully misdirected .....(specify the electronic message).....meant for .....(name the complainant).....

4.17 Charges Relating to Cyber Terrorism

4.17.1 CYBER TERRORISM CONTRARY TO SECTION 33 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you .....(accessed/caused to be accessed)..... ....a (computer/computer system/network) for purposes of carrying out a terrorist act namely..... (specify the terrorist act as per the Prevention of Terrorism Act, Cap 59B).....

4.18 Charges Relating to Inducement to Deliver Electronic Message

4.18.1 INDUCEMENT TO DELIVER ELECTRONIC MESSAGE CONTRARY TO SECTION 34 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you induced .....(name the person induced).....who was in charge of .....(specify the electronic device)..... to deliver an electronic message .....(specify the electronic message).....not specifically meant for ..... (name the accused).....

4.19 Charges Relating to Intentionally Withholding Message Delivered Erroneously

4.19.1 INTENTIONALLY WITHHOLDING MESSAGE DELIVERED ERRONEOUSLY CONTRARY TO SECTION 35 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you intentionally.....{(hid or detained) .....(electronic mail/message/electronic payment/credit and debit card)}..... which you ..... (found or delivered to you in error).....and which ought to be delivered to .....(specify the recipient/complainant).....

4.20 Charges Relating to Unlawful Destruction of Electronic Messages

4.20.1 UNLAWFUL DESTRUCTION OF ELECTRONIC MESSAGES CONTRARY TO SECTION 36 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you unlawfully.....(destroyed or aborted)..... .....(specify the electronic mail or processes through which money or information was conveyed).....

4.21 Charges Relating to Wrongful Distribution of Obscene or Intimate Images

4.21.1 WRONGFUL DISTRIBUTION OF OBSCENE OR INTIMATE IMAGES CONTRARY TO SECTION 36 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....you.....{*(transferred/published/ disseminated/ made a digital depiction available for distribution /downloading)* through a telecommunications network namely through .....*(specify the telecommunication network)*/ (*specify any other means of transferring data)*}..... to a computer, the intimate or obscene image of .....*(name the person)*.....

4.22 Charges Relating to Fraudulent Use of Electronic Data

4.22.1 FRAUDULENT USE OF ELECTRONIC DATA CONTRARY TO SECTION 38 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you knowingly and without authority caused the loss of.....(specify the property)..... belonging to.....(specify the person who suffers the loss).....by..... (altering/erasing/inputting/suppressing) data stored in a .....(specify the computer by indicating the serial number and make).....

4.22.2 FRAUDULENT USE OF ELECTRONIC DATA CONTRARY TO SECTION 38 (2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you sent an electronic message which materially misrepresented (Specify the fact misrepresented) which ..... (Name of the person who suffers loss) relied upon causing the said..... (Name of the person who suffers damage or loss) to suffer ..... (Specify the nature of damage or loss) .....

4.22.3 FRAUDULENT USE OF ELECTRONIC DATA CONTRARY TO SECTION 38 (3) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....with intent to defraud {(Franked electronic messages/instructions)/(subscribed any electronic messages/instructions)} .....(Specify electronic message/instructions).....

4.22.4 FRAUDULENT USE OF ELECTRONIC DATA CONTRARY TO SECTION 38 (4) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....you manipulated (a computer or other electronic payment device).....(Specify the computer or electronic device) ..... with the intent to..... (short pay/overpay) .....by Kshs..... (Specify the amount) .....

4.23 Charges Relating to Issuance of False E-Instructions

4.23.1 ISSUANCE OF FALSE E-INSTRUCTIONS CONTRARY TO SECTION 39 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location)..... being a person authorized to use a (computer or other electronic devices)..... (Specify the computer/device) ..... for financial transactions (including posting of debit and credit transactions/issuance of electronic instructions) as relates to (sending of electronic debit and credit messages/confirmation of electronic fund transfer) issued false electronic instructions..... (Specify the false instructions) .....

4.24 Charges Relating to Failure to Report a Cyber Threat

4.24.1 FAILURE TO REPORT A CYBER THREAT CONTRARY TO SECTION 40 (4) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location)..... being the person operating .....(Specify the type of computer system/network)..... failed to immediately inform the National Computer and Cybercrimes Coordination Committee of.....(Specify any attacks, intrusions/other disruptions) .....to the functioning of the said computer system or network within twenty-four hours of such (attack/intrusion/disruption).

4.25 Charges Relating to Failure by an Employee to Relinquish Access Codes

4.25.1 FAILURE BY AN EMPLOYEE TO RELINQUISH ACCESS CODES CONTRARY TO SECTION 41 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location)..... being a former employee of (Specify the employer)..... failed to relinquish all codes and access rights to (Specify the former employer's computer network/system) immediately upon termination of your employment.

4.26 Charges Relating to Aiding and Abetting

4.26.1 AIDING OR ABETTING (SPECIFY THE OFFENCE) CONTRARY TO SECTION 42 (1) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*..... you knowingly and willfully aided/abetted ..... *(Specify the offense)*.....

4.26.2 ATTEMPTED (SPECIFY THE OFFENCE) CONTRARY TO SECTION 42 (2) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location)..... you knowingly and willfully attempted ..... (Specify the offense).....

4.27 Charges Relating to Exercise of Powers of Search and Seizure

4.27.1 OBSTRUCTING THE LAWFUL EXERCISE OF POWERS GRANTED BY A WARRANT CONTRARY TO SECTION 48 (5) (a) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location)..... you obstructed the lawful exercise of the powers of an authorized person/police officer..... (Specify number, rank/designation and name).....granted pursuant to.....(Specify the particulars of the warrant).....by .....(Specify act of the obstruction).....

4.27.2 COMPROMISING THE INTEGRITY/CONFIDENTIALITY OF A COMPUTER SYSTEM/DATA/INFORMATION ACCESSED/RETAINED CONTRARY TO SECTION 48 (5) (b) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*..... you compromised the integrity or confidentiality of.....*(Specify the computer system/data/information accessed/retained)* ..... despite being presented with a warrant ..... *(describe the particulars of the warrant)* .....

4.27.3 MISUSE OF POWERS CONTRARY TO SECTION 48 (5) (c) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....being.....*(Description of the accused person)*....., granted pursuant to a warrant.....*(describe the particulars of the warrant)*..... you misused powers granted to you by.....*(Specify the misuse)*.....

4.28 Charges Relating to Section 52 of the CMCA

4.28.1 FAILURE TO COMPLY WITH A COURT ORDER CONTRARY TO SECTION 52 (7) OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....*(date)*.....at.....*(location)*.....being *(a service provider/principal officer of a service provider)*.....*(Specify the service provider)* ..... you failed to comply with an order..... *(order dated, issued by or other unique specifications)* .....

4.29 Charges Relating to Section 53 of the CMCA

4.29.1 FAILURE TO COMPLY WITH A COURT ORDER CONTRARY TO SECTION 53 (7) THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....being (a service provider/an officer of a service provider).....(Specify the service provider) ..... you failed to comply with an order..... (order dated, issued by or other unique specifications).....

4.30 Charges Relating to Obstruction or Misuse of Investigation Powers

4.30.1 OBSTRUCTION OF LAWFUL INVESTIGATIONS CONTRARY TO SECTION 54 (1) THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....being (Describe the person)..... you obstructed ..... (Specify the person obstructed) .....from lawful exercise of investigative powers by..... (Specify the nature of obstruction) .....

4.30.2 MISUSE OF INVESTIGATIVE POWERS CONTRARY TO SECTION 54 (2) THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

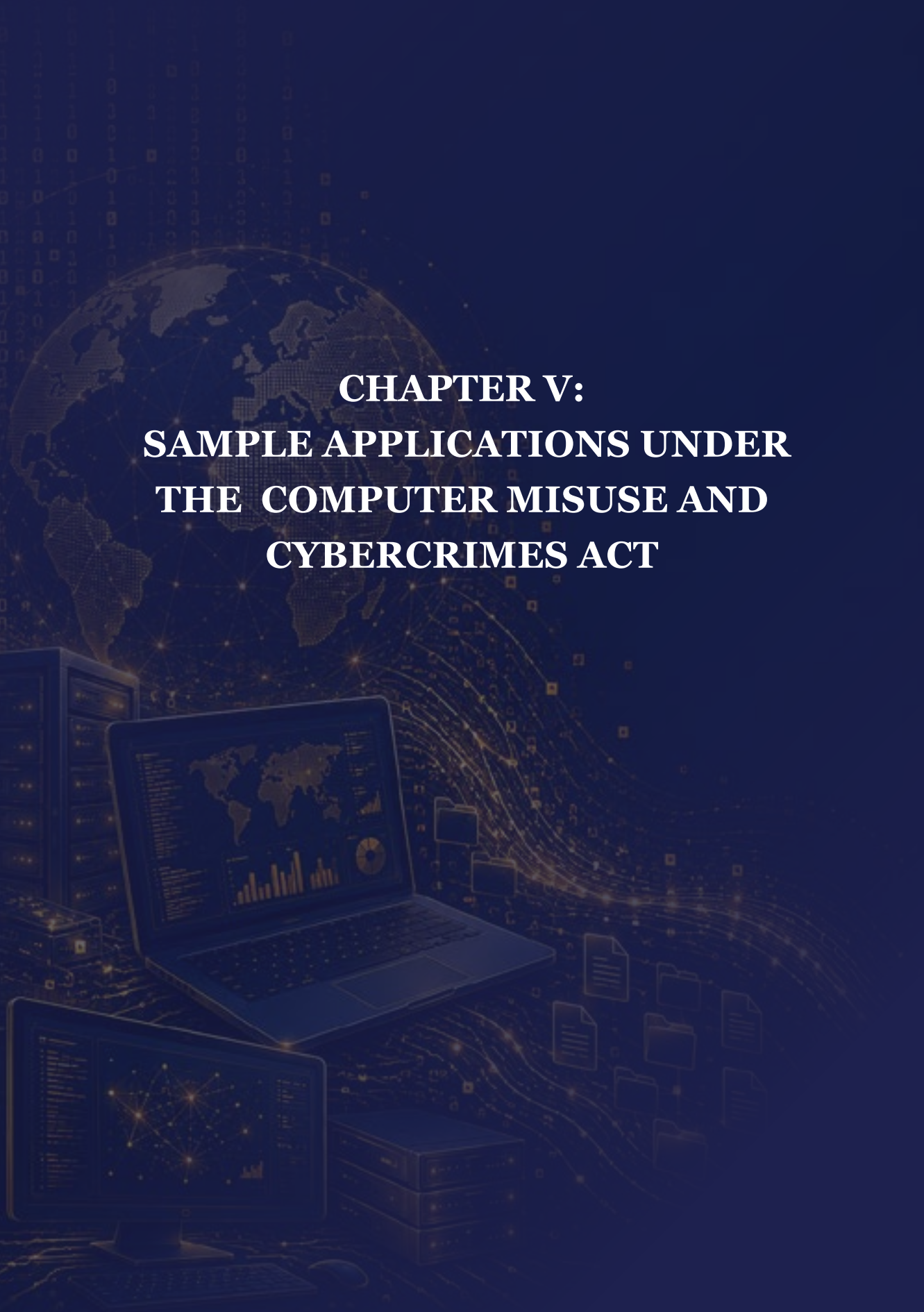
PARTICULARS OF OFFENCE

..... (accused 1)

..... (accused 2)

..... (*Any other)*

On.....(date).....at.....(location).....being.....(police officer/authorized person).....you..... (Specify the nature of misuse) .....



CHAPTER V:
SAMPLE APPLICATIONS UNDER THE COMPUTER MISUSE AND CYBERCRIMES ACT

CHAPTER V

SAMPLE APPLICATIONS UNDER THE COMPUTER MISUSE AND CYBERCRIMES ACT

Successful investigation and prosecution of cybercrimes is premised on a flawless chain of custody and digital trail. Because electronic evidence is inherently volatile, easily altered, and transnational in nature, the CMCA establishes robust, specialized procedural mechanisms to empower investigators to expeditiously access, preserve, seize, and intercept data. However, due to the intrusive nature of these investigative measures, especially their impact on the rights to privacy and property enshrined under Articles 31 and 40 of the Constitution of Kenya, the Act demands strict judicial oversight and meticulous adherence to statutory thresholds before these powers are deployed.

Moreover, the rapid dissemination of digital content requires swift judicial mechanisms capable of mitigating real time injury. Interim remedies therefore serve as vital safeguards against the compounding harm caused by cybercrimes. Section 27 (3) of the CMCA provides a crucial mechanism through protection orders, compelling an accused to immediately cease engaging in or facilitating Cyberharassment. By authorizing such interim relief, Section 27 (3) ensures that victims are protected from ongoing harm, during the pendency of the trial.

Section 46A complements this mechanism by authorising take down orders that compel the removal, deactivation or closure of computer systems, websites or digital devices that are used to promote unlawful activities, inappropriate sexual content of a minor, terrorism or religious extremism and cultism.

This Chapter provides standardized template applications designed to guide investigators and prosecutors through the various Applications under the CMCA. Crucially, these templates are not exhaustive or conclusive legal formulas, they should be adapted to fit the unique circumstances of each investigation. By utilizing them as a foundational guide, investigators and prosecutors can ensure protection of victims of cybercrime and lawful acquisition of evidence thus guaranteeing the effective investigation and prosecution of cybercrimes.

The Applications covered within this chapter are:

i. Application for a protection order under Section 27 (3) of the CMCA;

ii. Application for removal or restriction of unlawful online content pursuant to Section 46A (2) of the CMCA;

iii. Application for a search and seizure warrant under Section 48 of the CMCA;

iv. Application for a production order under Section 50 of the CMCA;

v. Application for expedited preservation and partial disclosure of traffic data under Section 51 of the CMCA;

vi. Application for real time collection of traffic data under Section 52 of the CMCA; and

vii. Application for realtime collection of content data under Section 53 of the CMCA

5.1 Section 27(3) CMCA: Application for a Protection Order in Cyber Harassment Cases

REPUBLIC OF KENYA

IN THE MAGISTRATE'S COURT AT [_____]

CRIMINAL CASE NO. _____ OF 20__

REPUBLIC/ INTERMEDIARY/ VICTIM .....APPLICANT

VERSUS

[NAME OF ACCUSED] ..... RESPONDENT

NOTICE OF MOTION

(Brought under Section 27(3)–(7) of the Computer Misuse and Cybercrimes Act, Cap 79C and Article 24 and 50 of the Constitution of Kenya)

TAKE NOTICE that this Honorable Court will be moved on the _____ day of _____, 20__ at [time] o'clock in the forenoon/afternoon, or so soon thereafter as counsel/the applicant may be heard, for **ORDERS THAT**:

1. This application be certified urgent and heard ex parte in the first instance.
2. A protection order do issue directing the Respondent/ accused to refrain, whether personally or through any other person, from engaging or attempting to engage in (describe the relevant conduct which the orders are being sought against.)
3. Any other or further order this Honorable Court may deem fit to grant.

WHICH APPLICATION is based on the following grounds, on th grounds set out in the Affidavit of [name] in support of the application and any other grounds to be adduced during the hearing thereof:

1. The Respondent has engaged in communication directed at the victim..... (describe the relevant conduct which the orders are being sought against.)
2. The communication is unwanted .....(further describe the communication as espoused under section 27 (1) (a) (b) or c of the CMCA, and its effect on the victim)
3. It is in the interests of justice that the reliefs sought be granted.

DATED at _____ this _____ day of _____, 20__.

_____

APPLICANT / INTERMEDIARY/ VICTIM (Choose the relevant one)

NB: This application should be accompanied with a Certificate of urgency, an affidavit in support of the Application and any other annextures. The application can be made outside court working hours pursuant to Section 27 (6) of the CMCA.

5.2 Section 46A (2) of the CMCA: Application for Removal or Restriction of Unlawful Online Content

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATE'S COURT AT [_____]

MISCELLANEOUS APPLICATION NO. _____ OF 20__

REPUBLIC..... APPLICANT

VERSUS

INTERNET SERVICE PROVIDER/ SOCIAL MEDIA PLATFORM..... RESPONDENT

COMMUNICATION AUTHORITY/KENIC.....INTERESTED PARTY

NOTICE OF MOTION

(Brought under Section 46A (2) of the Computer Misuse and Cybercrimes Act, Cap 79C, Article 24, 50 of the Constitution of Kenya)

TAKE NOTICE that this Honorable Court shall be moved on the _____ day of _____, 20__ at [time] o'clock in the forenoon/afternoon, or so soon thereafter as counsel/the applicant may be heard, for ORDERS THAT:

1. This application be certified urgent and heard ex parte in the first instance.
2. This Honourable Court be pleased to issue an order compelling the Respondent to remove [*describe the specific content and/ or material*] from [*describe the specific computer system/ website or digital device*] within [*indicate a specific time period*]; AND/ OR (select as appropriate)
3. This Honourable Court be pleased to issue an order for closure or deactivation of the [*describe the specific computer system, website or digital device*].
4. This Honourable Court be pleased to issue such orders as may be necessary for the ends of justice to be met.

WHICH APPLICATION is based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof:

1. There is a basis to believe that [*specify the computer system, website or digital device*] is being used to promote [*unlawful activities/ inappropriate sexual content of a minor/ terrorism/ religious extremism and cultism*] (select as appropriate);
2. The removal of the .....[*specify the content*], rather than restriction of the entire platform, ...[is or is not].... sufficient to address the harm as [*describe why restriction is not sufficient to address the harm].*
3. The following steps have been taken to notify the operator..... of these/ intention to institute these proceedings.
4. It is in the interest of justice that the reliefs sought be granted.

DATED at _____ this _____ day of _____, 20__.

_____

APPLICANT

5.3 Section 48: CMCA: Application for a Search and Seizure Warrant

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATE'S COURT AT .....

MISCELLANEOUS CRIMINAL APPLICATION NO. ..... OF 2026

IN THE MATTER OF AN APPLICATION FOR A WARRANT PURSUANT TO SECTION 48 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT,CAP 79C

BETWEEN

DIRECTORATE OF CRIMINAL INVESTIGATIONS (DCI)..... APPLICANT

AND

[NAME OF RESPONDENT] .....RESPONDENT

NOTICE OF MOTION

(Article 24 of the Constitution, Section 48 of the Computer Misuse and Cybercrimes Act, Cap 79C, Section 75 of the Evidence Act, Cap 80, Section 118 and 118A of the Criminal Procedure Code)

TAKE NOTICE THAT this honourable court shall be moved on the ..... Day of .....at 9.00 o'clock in the forenoon or soon thereafter in the forenoon or soon thereafter where the applicant shall be heard for ORDERS THAT:

1. This application be certified urgent and be heard heard ex parte in the first instance
2. The court be pleased to issue a Warrant authorizing *[Insert Name, Rank, and Force Number of the Investigating Officer*], a police officer attached to [*Insert Unit],* to enter the premises located at [*Insert Exact Physical Address/Description of Target Location*] occupied by [*insert name of target individual/company*].
3. The said officer or any other authorized person assisting them be permitted to access, search, examine, copy, and seize *[specify the computer system/ items]* found on the premises or in possession of persons therein.
4. The respondent, their employees, agents, or any person in charge of the specified computer systems be compelled to cooperate with .....[specify the name and rank of officer] while undertaking the lawful search and seizure of the [*specify the subject of the search].*

WHICH APPLICATION is based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof:

1. **THAT** the Applicant is conducting an investigation into the commission of an offence under the Computer Misuse and Cybercrimes Act.
2. **THAT** preliminary investigations reveal that the suspect(s) utilized a computer system to [*Briefly state the outcome of preliminary investigations].*
3. **THAT** electronic footprints and IP address tracking point directs to a computer system and data storage mediums currently housed at the premises of the Respondent located at [*give a description of location*].
4. **THAT** I have reasonable grounds to believe that the data, computer programs, and storage devices contained in the aforementioned premises are material evidence necessary for the successful investigation of the above mentioned complaint.
5. **THAT** unless this application is granted ex-parte without prior notification to the Respondent, there is a real and imminent danger that the targeted digital evidence will be permanently deleted, encrypted, or wiped clean, thereby defeating the ends of justice.

6. **THAT** this application has been made in good faith.
7. **THAT** this honourable Court is seized with jurisdiction to issue a warrant directing a police officer to enter, search, and seize such data.
8. **THAT** it is in the interest of justice that the said orders be granted as prayed.

Dated at ..... this..... day of.....20.....

PROSECUTION COUNSEL

FOR: THE DIRECTOR OF PUBLIC PROSECUTIONS

DRAWN AND FILED BY:

Office of the Director of Public Prosecutions,

ODPP House, Ragati Road, Upper Hill.

P.O. BOX 30701 – 00100,

NAIROBI

Email: info@odpp.go.ke.

TO BE SERVED UPON:

The Respondent

NB.

i. The warrant must explicitly name the electronic items or the specific computer systems you want to search. Broad, vague requests are frequently thrown out by magistrates.

ii. Once the warrant is issued, the executing officer must present a physical copy of the warrant to the person against whom it is issued (Section 48(4)).

iii. Immediately after execution, the officer is legally required under Section 49 to compile a complete, signed inventory of every system, phone, or laptop seized or rendered inaccessible, providing a direct copy to the occupier of the premises.

5.4 Section 50: Application for a Production Order

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATES COURT AT NAIROBI

MILIMANI LAW COURTS

MISCELLANEOUS CRIMINAL APPLICATION NO.....

IN THE MATTER OF AN APPLICATION FOR PRODUCTION ORDER UNDER SECTION 50 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

THE DIRECTORATE OF CRIMINAL INVESTIGATIONS.....APPLICANT

VERSUS

[BANK/ SERVICE PROVIDER/ VASP] .....RESPONDENT

NOTICE OF MOTION

(Article 24 of the Constitution of Kenya, Section 50 of the Computer Misuse and Cybercrimes Act, CAP 79C, Section 118, 118A and Section 121 of Criminal Procedure Code, CAP 75 and Section 180 of the Evidence Act Cap 80 and all other enabling laws of Kenya)

TAKE NOTICE THAT this honourable court shall be moved on the ..... Day of .....at 9.00 o'clock in the forenoon or soon thereafter in the forenoon or soon thereafter where the applicant shall be heard for ORDERS THAT:

1. This Application be certified as urgent and be heard ex parte in the first instance.
2. The Respondent be ordered to submit and produce the following specified computer data or subscriber information currently in their possession or control:
    a. [e.g., KYCs and account opening documents for Account No. XXXXXX].
    b. [e.g., Full transaction history including IP logs for the period between specify period].
    c. [e.g., Associated recovery email addresses and phone numbers].
3. The said data be produced in a [*Specify Format: e.g., Digitally signed PDF or Excel spreadsheet]* and delivered to [*specify the name and rank of the intended receipient of the data*] expeditiously upon service of this order.
4. The said data be accompanied with a certificate of electronic evidence duly signed by the Respondent or any other authorised officer.
5. The Respondent be prohibited from disclosing the existence of this application or order to the account holder or any third party.

WHICH APPLICATION is based based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof**:**

1. THAT the Applicant is investigating the offence of [*State Offence*] and has reasonable grounds to believe the Respondent holds data (*specify the data sought*) necessary for the investigation.

2. **THAT** preliminary investigations reveal that the suspect(s) utilized a computer system to [*Briefly state the outcome of preliminary investigations*].
3. **THAT** the Respondent is a designated data controller/service provider in Kenya and is legally bound to comply with lawful production orders issued by a court of competent jurisdiction.
4. **THAT** the ..... (specify the data/ information sought) is stored in a computer system or storage medium within the possession and control of the Respondent.
5. **THAT** the production of this information is desirable and necessary for the purposes of the investigation to [*specify purpose eg identify the perpetrator or trace proceeds of crime*.]
6. **THAT** unless this application is granted ex-parte without prior notification to the Respondent, there is a real and imminent danger that the data subject might be alarmed or triggered into taking actions that might undermine the ends of justice.
7. **THAT** the Application is made in good faith.
8. **THAT** it is in the interest of justice that the Application be granted as prayed.

Dated at NAIROBI this..... day of.....20.....

PROSECUTION COUNSEL

FOR: THE DIRECTOR OF PUBLIC PROSECUTIONS

DRAWN AND FILED BY:

Office of the Director of Public Prosecutions,

ODPP House, Ragati Road, Upper Hill.

P.O. BOX 30701 – 00100,

NAIROBI

Email: info@odpp.go.ke.

5.5 Section 51: Application for Expedited Preservation and Partial Disclosure of Traffic Data

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATES COURT AT .....

MISCELLANEOUS CRIMINAL APPLICATION NO.....

IN THE MATTER OF AN APPLICATION FOR EXPEDITED PRESERVATION AND PARTIAL DISCLOSURE OF TRAFFIC DATA

UNDER SECTION 51 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

THE DIRECTORATE OF CRIMINAL INVESTIGATIONS .....APPLICANT

VERSUS

[SERVICE PROVIDER] .....RESPONDENT

NOTICE OF MOTION

(Article *24, of the Constitution of Kenya, Section 51 of the Computer Misuse and Cybercrimes Act, CAP 79C, Section 118 and section 121 of Criminal Procedure Code, CAP 75 and Section 180 of the Evidence Act Cap 80, & all other enabling laws of Kenya)*

TAKE NOTICE THAT this honourable court shall be moved on the ..... Day of .....at 9.00 o'clock in the forenoon or soon thereafter in the forenoon or soon thereafter where the applicant shall be heard for ORDERS THAT:

1. This Application be certified as urgent and be heard ex parte.
2. The Respondent be and is hereby directed to expeditiously preserve/ disclose all available (*specify the data that is to be preserved/ disclosed*] associated with [Phone Number / IP Address / Account ID] for a period of thirty (30) days regardless of whether one or more service providers were involved in the transmission of that communication.
3. The Respondent be directed to maintain the integrity of the data specified in (2) above and ensure it is not modified, lost, or destroyed.
4. The Respondent be compelled to disclose to the Applicant sufficient [*specify the traffic data to be disclosed*] concerning any communication in order to identify the service providers and the path through which communication was transmitted.
5. The Respondent be prohibited from disclosing the existence of this order to the subscriber or any third party for the duration of the preservation period.

WHICH APPLICATION is based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof:

1. **THAT** the Applicant is investigating the commission of a cybercrime involving [*briefly describe the nature of crime under investigation].*
2. **THAT** on .....day....of ....Month.....20.... a notice was served to the Respondent requiring the expedited preservation of ...(*specify the data preserved*) for a period of thirty (30) days.

3. **THAT** upon serving the notice of the expedited preservation of the *(specify the data preserved*), the Applicant has undertaken investigations to wit ...(*specify the investigative steps and briefly describe the outcomes of the investigation*).....
4. **THAT** the period for which the Respondent can possibly preserve the said data without a court order has since lapsed yet the investigations are yet to be completed due to ..... (*explain the difficulty encountered in completing investigations within the thirty-day period*).
5. **THAT** there is therefore need to extend the preservation for a further..... (specify the duration of extension sought) days to facilitate effective investigations into the alleged criminal conduct.
6. **THAT** there is an imminent risk or vulnerability that the traffic data, subject of this application, may be modified, lost, destroyed or rendered inaccessible if the reliefs sought are not granted. Thus undermining the outcome of investigations.
7. **THAT** the cost of the extended preservation orders is not overly burdensome on the Respondents.
8. **THAT** disclosure of the existence of this application to the data subjects or any other party other than the Applicant or its authorized officer prior to effecting the preservation might undermine the outcome of the investigations.
9. **THAT** the orders sought are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.
10. **THAT** the orders sought are proportionate to the intended purpose of countering crime and maintaining law and order.
11. **THAT** this application has been made in good faith.
12. **THAT** this honourable court has jurisdiction to grant the reliefs sought
13. **THAT** it is reasonable and in the interest of justice that the orders be granted as prayed.

Dated at NAIROBI this..... day of.....2026

PROSECUTION COUNSEL

FOR: THE DIRECTOR OF PUBLIC PROSECUTIONS

DRAWN AND FILED BY:

Office of the Director of Public Prosecutions,

ODPP House, Ragati Road, Upper Hill.

P.O. BOX 30701 – 00100,

NAIROBI

Email: info@odpp.go.ke.

TO BE SERVED UPON:

The Respondent

5.6 Section 52: Application for Real-Time Collection of Traffic Data

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATES COURT AT .....

MISCELLANEOUS CRIMINAL APPLICATION NO.... OF 20....

IN THE MATTER OF AN APPLICATION FOR REAL TIME COLLECTION OF TRAFFIC DATA UNDER SECTION 52 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

THE DIRECTORATE OF CRIMINAL INVESTIGATIONS .....APPLICANT

VERSUS

XXXXXX..... RESPONDENT

NOTICE OF MOTION

(Article 24 of the Constitution of Kenya, Section 52 of the Computer Misuse and Cybercrimes Act, CAP 79C, Section 118 and section 121 of Criminal Procedure Code, CAP 75 and Section 180 of the Evidence Act Cap 80 and & all other enabling laws of Kenya)

TAKE NOTICE THAT this honourable court shall be moved on the ..... Day of .....at 9.00 o'clock in the forenoon or soon thereafter in the forenoon or soon thereafter where the applicant shall be heard for ORDERS THAT:

1. This Application be certified as urgent and be heard ex parte.
2. The Applicant be authorized to collect or record, through the application of technical means, traffic data in real-time associated with specified communications from [*Target Account/IP Address/Device*] for a period of ..... (*specify the duration sought but not exceeding six months*) days.
3. The Respondent be compelled to cooperate and assist the Applicant or any other authorised person in the said real-time collection or recording of the .....[*specify the communication subject of the application*] transmitted by means of a computer system.
4. The Respondent be ordered to keep this application and the resulting order strictly confidential to avoid alerting the data subject of the existence of this order or application.

WHICH APPLICATION is based on is based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof:

1. **THAT** there are reasonable grounds to believe that real-time traffic data from ...(*describe the computer system from which the traffic data is sought*) is within the possession or control of the Respondent.
2. **THAT** there are reasonable grounds to believe that the specified computer system has data relating to (*identify and explain, the type of traffic data suspected to be found on such computer system*)
3. **THAT** there are reasonable grounds to believe that the target computer system [*insert IP/Server/Device details*] is currently being utilized by [*insert suspect name/alias or 'unknown user operating unique identifier X'*] to facilitate an offence. The requested real-time collection of traffic data is strictly necessary to identify the subscriber and trace the active user session associated with the specified unique identifiers across the network.

4. **THAT** specific, identifiable offences under [*insert relevant Act sections and describe the offences*] have been committed, are currently being committed, or are reasonably suspected to be in preparation using the target computer system, thereby establishing the statutory threshold for real-time traffic data collection.
5. **THAT** the extent of the collection is commensurate and proportionate, as traditional production of historical data under Section 50 of the Computer Misuse and Cybercrimes Act is insufficient since..... *(justify why real time collection is the only necessary mechanism available for effective investigation of the offence/ complaint.)*
6. **THAT** the Applicant has put in place necessary procedural, technical, and operational safeguards to ensure that the collection of real-time traffic data is strictly targeted; specifically ensuring that:
    i. The privacy of uninvolved third parties, customers, and general system users is maintained through precise filtering and minimization protocols; and
    ii. The acquired traffic data remains confidential and is protected against disclosure to any entity or individual not officially participating in the underlying investigation.
7. **THAT** unless this honourable court grants the reliefs sought, the investigation may be frustrated or seriously prejudiced.
8. **THAT** the cost of grant of the reliefs sought is not overly burdensome upon the person in control of the computer system.
9. **THAT** it is in the interest of justice that the orders be granted as prayed.

Dated at NAIROBI this..... day of.....2026

PROSECUTION COUNSEL

FOR: THE DIRECTOR OF PUBLIC PROSECUTIONS

DRAWN AND FILED BY:

Office of the Director of Public Prosecutions,

ODPP House, Ragati Road, Upper Hill.

P.O. BOX 30701 – 00100,

NAIROBI

Email: info@odpp.go.ke.

NB: The court may grant an extension of the reliefs granted for more than six months pursuant to Section 52 (6) of the CMCA.

5.7 Section 53: Application for Interception of Content Data

REPUBLIC OF KENYA

IN THE CHIEF MAGISTRATES COURT AT .....

MISCELLANEOUS CRIMINAL APPLICATION NO.....

IN THE MATTER OF AN APPLICATION FOR INTERCEPTION OF CONTENT DATA UNDER SECTION 53 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT, CAP 79C

THE DIRECTORATE OF CRIMINAL INVESTIGATIONS..... APPLICANT

VERSUS

XXXXXX.....RESPONDENT

NOTICE OF MOTION

(Article 24 of the Constitution of Kenya, Section 53 of the Computer Misuse and Cybercrimes Act, CAP 79C, Section 118 and section 121 of Criminal Procedure Code, CAP 75 and Section 180 of the Evidence Act Cap 80 and & all other enabling laws of Kenya)

TAKE NOTICE THAT this honourable court shall be moved on the ..... Day of .....at 9.00 o'clock in the forenoon or soon thereafter in the forenoon or soon thereafter where the applicant shall be heard for ORDERS THAT:

1. This Application be certified urgent and be heard ex parte and in camera.
2. The Applicant be permitted to collect or record, through technical means, the content data of (*describe the specifically identified electronic communications*) from [*Target Account/ Device/Identifier*].
3. The Respondent be compelled to co-operate and assist the Applicant in the real-time collection or recording of the said content data transmitted by means of a computer system for a period not exceeding [*Specify Period but noit exceeding nine months*].
4. The Respondent be prohibited from disclosing the existence of this order or the ongoing interception to the data subject or any third party.

WHICH APPLICATION is based on is based on the following grounds, on the grounds set out in the Affidavit of [.....], in support of the application and on such other grounds to be adduced at the hearing thereof:

1. **THAT** there are reasonable grounds to believe the target content data is within the control, custody, or active infrastructure of *[Insert Name of Service Provider / Entity in Control*], as the said entity hosts, transmits, or processes the electronic communications originating from and directed to the target computer system *[Insert IP / Account Details].*
2. **THAT** the real-time collection or recording is strictly limited to specified categories of content data; namely [*identify and state the type of content data suspected to be found on such computer system*]; which are currently being transmitted through or stored upon the subject computer system.
3. **THAT** the order is sought in respect of specific, identifiable offences; namely [*Insert*

Offence(s)]; which have been committed, are actively being executed, or are imminently threatened using the specified computer system.

4. **THAT** the applicant has the statutory authority to seek real-time collection of content data, and that continuous or multiple disclosures across [*Insert specified duration e.g., ... days*] are strictly necessary because [*justify the need for real time collection of content data over the duration sought*] to achieve the objective of the warrant.
5. **THAT** robust procedural and technical measures have been established to ensure that the collection of content data is strictly targeted, thereby:
    i. Maintaining the privacy of non-subject users, customers, and third parties through targeted packet/session filtering and data minimization; and
    ii. Protecting all captured data from unauthorized disclosure to any party outside the official investigative and prosecutorial team.
6. **THAT** the Respondent has the technical capability to comply with the orders sought as the cost of such real-time recording and collection is not overly burdensome upon the Respondent.
7. **THAT** unless real time collection or recording of content data is urgently granted, the ongoing investigation will be frustrated or seriously prejudiced, as the volatile nature of the communications allows critical evidence to be altered, deleted, or permanently lost upon session termination.
8. **THAT** the real-time collection or recording shall be executed by [*state the manner in which they shall achieve the objective of the warrant, real time collection or recording by the person in control of the computer system where necessary*] to securely capture and deliver the data without compromising system integrity.
9. **THAT** other less intrusive investigative measures have been exhausted and have proven futile as the target account *(describe why less intrusive means have been unsuccessful)*
10. **THAT** measures have been taken to protect the privacy of innocent third parties.
11. **THAT** it is in the interest of justice that the orders sought be granted as prayed.

Dated at NAIROBI this..... day of.....2026

PROSECUTION COUNSEL

FOR: THE DIRECTOR OF PUBLIC PROSECUTIONS

DRAWN AND FILED BY:

Office of the Director of Public Prosecutions,

ODPP House, Ragati Road, Upper Hill.

P.O. BOX 30701 – 00100,

NAIROBI

Email: info@odpp.go.ke.

NB: The court may grant an extension of the reliefs granted for more than nine months pursuant to Section 53 (5) of the CMCA.

5.8 Guidance Note on Real-Time Collection Orders for Traffic and Content Data (Sections 52 & 53, CMCA)

Both Applications under Section 52 and 53 of the Act may be extended beyond the statutory limit of sicx months and nine months respectively if the court is satisfied that:

i. **Investigative or Prosecutorial Necessity:** The extension is reasonably required to advance an ongoing investigation or support a prosecution.
ii. **Proportionality & Suitability**: The scope and extent of the requested extension are proportionate, commensurate, and strictly necessary for the purpose of the case.
iii. **Unfulfilled Warrant Purpose:** Despite prior authorization, further collection remains necessary to achieve the specific objectives for which the initial warrant was issued.
iv. **Third-Party Privacy & Data Safeguards:** Measures remain actively in place to protect privacy of third parties and prevent unauthorized disclosure to persons outside the investigation.
v. **Risk of Prejudice:** The investigation would be frustrated, compromised, or seriously prejudiced if the extension were refused.
vi. **Reasonable Burden on Service Providers:** The operational or financial cost imposed on the person in control of the computer system (e.g., service provider) is not overly burdensome.

Given the covert and highly intrusive nature of real-time data collection, protecting the operational integrity of the investigation is critical. Investigators and prosecutors must ensure these applications are shielded from the public domain to prevent tipping off the suspect or exposing sensitive surveillance methods.

A Chamber Summons Application may be filed as a precursor to the Application under Section 52 or 53 of the CMCA bearing in mind the following:

i. **File Ex Parte:** Applications for real-time collection must inherently be filed ex parte (without notice to the respondent or target). Alerting the suspect defeats the purpose of the application.
ii. **Seek in Camera Hearing**: Explicitly include a prayer in the application requesting the judicial officer to hear the matter in camera (in chambers or a closed courtroom). Do not file a standard open court application via the electronic filing system.
iii. **Justify the Secrecy:** Use your supporting affidavit to justify why an open hearing would prejudice the investigation. Cite the necessity of protecting covert law enforcement techniques and the statutory duty to safeguard the privacy of innocent third parties.
iv. **Apply to Seal the File:** Request an explicit court directive that the application file, supporting affidavits, and the resulting orders be sealed by the registry.
v. **Seek Non-Disclosure Orders**: Ensure the court order explicitly binds the internet or telecommunications service provider, and their employees, to strict confidentiality regarding the existence and execution of the warrant.

CHAPTER VI:
INTERNATIONAL COOPERATION

CHAPTER VI

INTERNATIONAL COOPERATION

Cybercrime is fundamentally transnational in nature. Threat actors operating from jurisdictions thousands of kilometres away can target and disrupt Kenya's national Critical Information Infrastructure or compromise financial systems within seconds. Unlike conventional crimes, cybercrimes transcend geographical boundaries, with digital evidence often dispersed across multiple countries and hosted on foreign servers. The speed, anonymity and transantional nature of cyberspace significantly complicates investigation, attribution and prosecution efforts, making international cooperation essential for effective cybercrime prevention, investigation and prosecution.

Part V of the CMCA provides Kenya's legal framework for international cooperation. Read alongside the Mutual Legal Assistance AWwct (Cap. 75A), Extradition (Commonwealth Countries) Act (Cap 77) and the Extradition (Contiguous and Foreign Countries) Act (Cap 76), this Part empowers Kenyan prosecutors and law enforcement to collaborate seamlessly with foreign jurisdictions to promptly freeze, preserve, and collect electronic evidence through diverse mechanisms.

6.1 Core Legal Mechanisms on International Cooperation

S/No	Mechanism	CMCA Provision	Operational Target	Scope & Limitations
1.	**Expedited Preservation of Stored Data**	**Section 59**	Fast-tracking the freeze of target data on a foreign or domestic server.	Secures data for a period of not less than one hundred and twenty days while a formal MLA request is drafted.
2.	**ExpediteWd Disclosure of Traffic Data**	**Section 60**	Identifying the path of specified communication across networks.	Limited strictly to traffic data (IP addresses, routing, timestamps) does not include communication content.
3.	**Real-Time Collection of Traffic Data**	**Section 63**	Tracking active, live digital footprints as they move across routers.	Relies on reciprocal treaty agreements and judicial authorisation.
4.	**Interception of Content Data**	**Section 64**	Accessing the actual substance of messages (e.g., chat logs, emails).	Subject to judicial authorisation and relies on reciprocal treaty agreements

6.2 Trans-Border Access to Public or Consensual Data (Section 62)

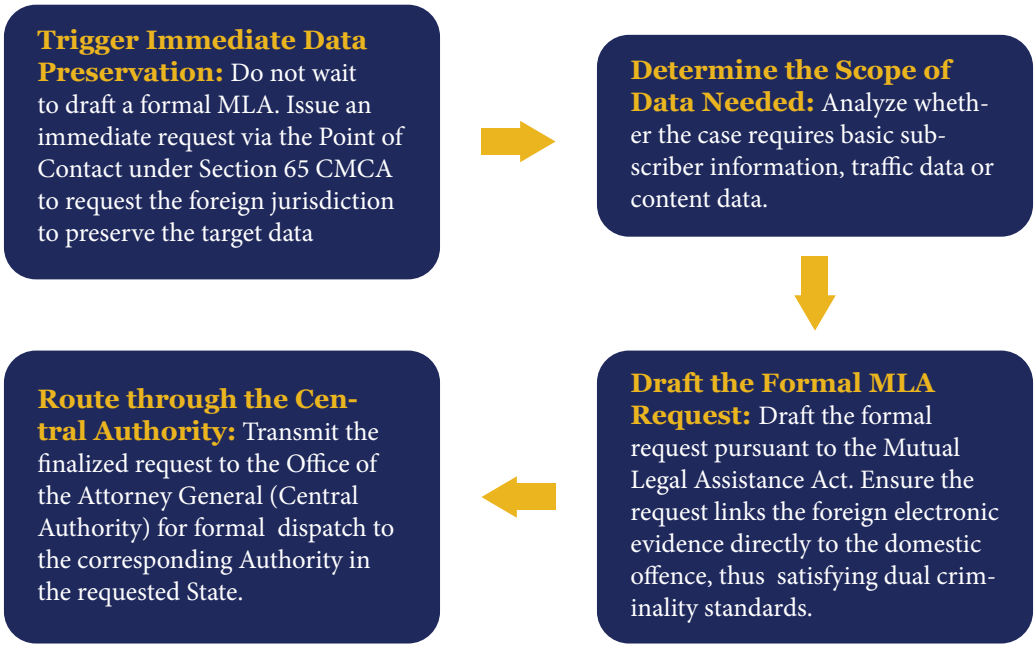
Due to the administrative delays inherent in traditional MLA requests, Section 62 allows law enforcement a more expeditious pathway to access cross-border data in two specific scenarios:

i. **Publicly Available Data:** If the data is stored in a foreign country but is publicly accessible (e.g., an open website or open-source database), it can be retrieved directly.

ii. **Consent of the Data Owner:** If a person or entity with lawful authority over the data gives voluntary, explicit consent, it can be accessed across borders without triggering formal diplomatic channels.

6.3 Protocol for International Assistance

When an investigation reveals that crucial electronic evidence is located outside Kenya, there is need to undertake the following systematic steps to ensure preservation of the said data:



6.4 Critical Checkpoints

When reviewing files involving foreign electronic evidence it is crucial to observe the following:

i. **Chain of Custody:** Is there clear documentation demonstrating the manner in which the data travelled from the foreign server or platform to the Kenyan investigators?

ii. **Admissibility under the Evidence Act:** Ensure compliance with Section 106B of the Evidence Act (Cap 80). Any foreign electronic record should be accompanied by a valid electronic certificate signed by the responsible foreign official or authorized service provider.

iii. **Data Privacy Compliance:** Verify that the request aligns with the Data Protection Act, CAP 411C, particularly regarding the transfer of personal data outside Kenya.

iv. **Specificity:** Clearly define the scope of the request (e.g., specific IP addresses, timestamps, and account identifiers).

6.5 Conclusion

International cooperation is indispensable in modern transborder cybercrime investigations. By leveraging these statutory mechanisms, investigators and prosecutors can swiftly secure volatile cross-border evidence while strictly adhering to essential legal safeguards. This dual approach ensures that foreign digital data is gathered rapidly to mitigate active threats and handled with the exact precision required to satisfy established admissibility standards in a court of law.

Contact us:

Office of the Director of Public Prosecution
ODPP House, Ragati Road, Upper Hill, Nairobi
P.O Box 30701- 00100

Tel: +254 2732090 / 2732240 | **Mobile:** 0723202880 / 0787880580
Fax: +254 2243524/2251808 | **Email:** info@odpp.go.ke

www.odpp.go.ke