Activity supported by the
Canada Fund for Local Initiatives
Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada

ELGIA
ELECTORAL LAW AND GOVERNANCE
INSTITUTE FOR AFRICA

COMPUTER MISUSE & CYBERCRIME ACT, 2018

ABRIDGED VERSION

Understanding risks, strengthening defenses and building safer systems.

Introduction

The Importance of Cyber Security

The Computer Misuse and Cybercrimes Act (CMC Act) was first passed in 2018 to determine offences relating to computer systems and networks facilitate timely and effective detection, prevention, response, investigation, and prosecution of computer and cybercrimes,

The act protects individuals, organizations, and governments from crimes committed using computers, mobile phones, and the internet. The CMCA Act, 2018 was amended in 2025 to address emerging threats like SIM-swap fraud and phishing; and regulate new digital spaces like virtual assets and digital accounts.

What are the Objectives of the CMC Act 2018?

The main objectives of the CMC Act, 2018 and the CMCA Amendment Act 2025 are:

- To prevent the unlawful use of computer systems
- To facilitate the prevention, detection, investigation, prosecution, and punishment of cybercrimes
- To protect the rights to privacy, freedom of expression, and access to information as per the Constitution of Kenya
- To protect the confidentiality, integrity, and availability of computer systems, programs, and data
- To help Kenya work with other countries to prevent, investigate, and punish computer misuse and cybercrimes across borders

Who Enforces the Act?

The responsibility of enforcing the CMC Act, 2018 and the CMCA Amendment Act 2025 lies with the National Computer and Cybercrimes Co-ordination Committee (NCCCC). Established by the CMC Act 2018, the Committee coordinates the fight against cybercrime and computer misuse in Kenya. The NCCCC comprises following top government officials or their representatives:

The Chairperson
An internal security representative responsible for leading and receiving reports from the NCCC Committee

The Director General of the Communications Authority
They regulate internet and communication services.

The Governor of the Central Bank of Kenya
They are in the committee to safeguard banks and the mobile money system.

The Director General of the National Intelligence Service
To identify cyber threats

The Chief of the Kenya Defense Forces
To offer national security support.

Inspector General of the Kenya Police
To enforce the law

The Director of Public Prosecution
To prosecute cyber crime cases

The Attorney General
To offer legal guidance to the committee.

The Director /Secretary
They are mandated to record decisions.

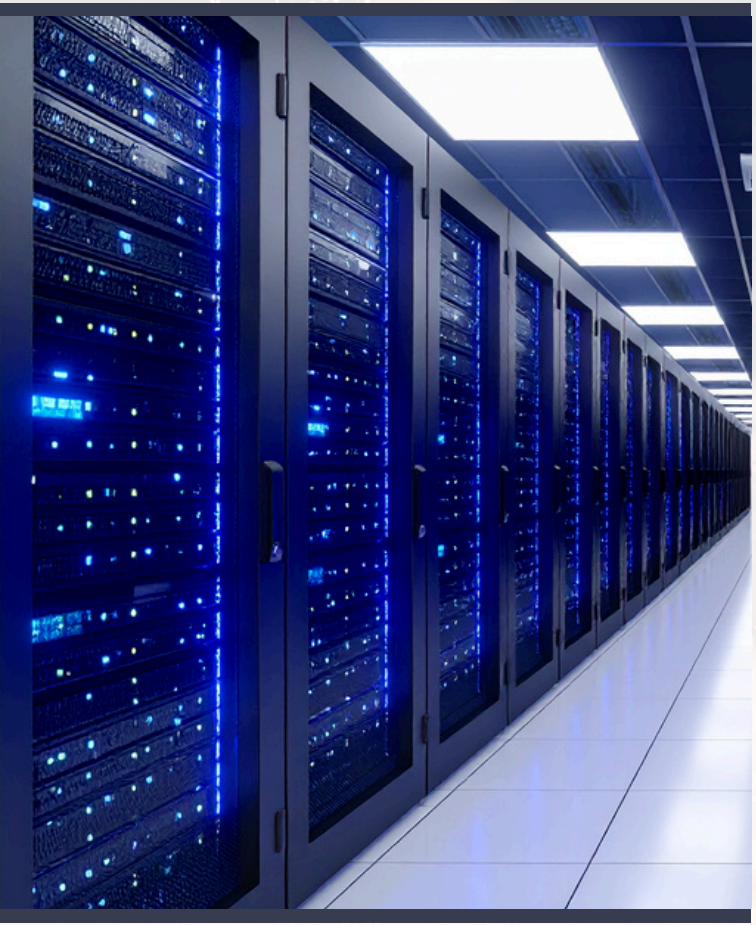
What are the Responsibilities of the NCCC Committee?

According to the CMC Act, 2018, the National Computer and Cybercrimes Co-ordination Committee is responsible for:

- Advising the government on ways to protect financial systems like mobile money, blockchain systems, and trust accounts
- Co-operating with computer incident response teams and other relevant bodies, locally and internationally to respond to threats of computer and cybercrime and incidents
- Protecting critical national data and systems to ensure that they remain private, accurate, and reliable
- Guiding national security leaders on cybercrime issues
- Ensuring that security agencies collaborate in addressing cybercrime
- Receiving reports about cybercrimes and taking relevant action
- Watching out for cyber threats and responding quickly to online attacks
- Setting up secure digital systems to ensure that online services are safe to use

Note

The NCCC Committee is required to submit quarterly reports to the National Security Council. The CMC Act, 2018 establishes a secretariat to support the NCCC Committee. This secretariat is headed by a Director and is responsible for the day to day administration and implementation of Committee decisions. The Act allows the Director to designate certain systems as critical infrastructure through a Gazette notice.

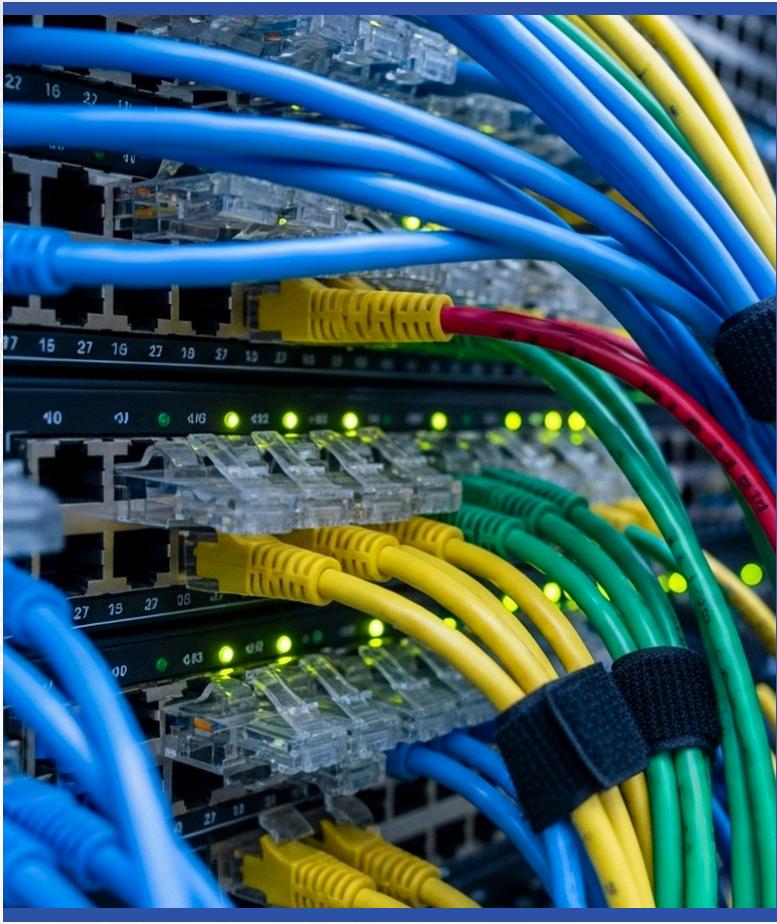


What is Critical Information Infrastructure Under the CMC Act 2018 ?

These are systems whose disruption would interrupt life sustaining services like supply of water, health services and energy. Disruption of such such systems could also affect the economy of the country adversely, result in an event that would cause massive casualties or fatalities, or lead to failure or substantial disruption of the money market of the Republic.

Upon gazetting a system as a critical infrastructure, the Director informs the owner or operator of the system the reasons for the designation within reasonable time and issues directives to regulate the:

- Management and protection of the system
- Classification, storage, and retrieval of data held in the system
- Management of cyber incidents
- Disaster recovery for the critical information infrastructure
- Minimum security measures to be applied
- Timeline for complying with the directives



How Should Critical Information Infrastructure be Protected?

To protect the critical information infrastructure, the National Computer and Cybercrimes Co-ordination Committee, in consultation with the owner or operator of the critical information infrastructure, undertake the following

- Conduct an assessment of the threats, vulnerabilities, risks, and probability of a cyberattack.
- Determine the harm to the economy if the system is compromised.
- Measure the overall level of preparedness against damage or unauthorized access.
- Identify any other risk-based security factors appropriate and necessary to protect public health and safety, or national socio-economic security; and
- Recommend to the owners of systems on methods of securing their systems against cyber threats

Reporting on Critical Information Infrastructure

The CMC Act provides that:

- Owners/operators of systems that are designated as critical information infrastructure report any suspected incidents of cyber and computer crime threats to the National Computer and Cybercrimes Co-ordination Committee
- The report should explain the actions the owner or operator intends to take to prevent the threat.
- The National Security Council will provide technical assistance based on the report to help reduce the threat.
- The Director shall independently investigate the cyber threats and take necessary actions to secure the infrastructure.
- The Director must submit a report on any reported cyber threat to the National Security Council.

Agreements on Critical Information Infrastructure

The CMC Act allows private entities to enter into information-sharing agreements with public entities on the critical information infrastructure for the following purposes:

01 To ensure cyber security.

02 For the investigation and prosecution of crimes related to cyber security.

03 For the protection of life or property of an individual.

04 To protect the national security of the country

Auditing of Critical Information Infrastructure

The CMC Act provides for regular auditing of critical information infrastructure to ensure compliance. Under the Act:

- Critical information infrastructure owners/operators must submit an annual compliance report to the National Computer and Cybercrimes Co-ordination Committee
- The Director must give a written notice before conducting an audit on a critical information infrastructure or any time there is an imminent cyber threat. The notice must indicate the date for the audit and the particulars and contact details of the person who is responsible for the overall management and control of the audit.
- The Director appoints persons to conduct audits on critical information infrastructure and provides oversight on the entire audit process.
- The Director may also request additional information to address audit findings
- Failing to submit annual reports, co-operate with audits, provide requested information, or obstructing auditors is an offence punishable by a fine of up to Kshs. 200,000, imprisonment of up to five years, or both.

What are the Main Offences and Penalties in the CMC Act 2018?

Offence	Description	Penalty
Unauthorized access	Involves causing a computer system to perform a function temporarily or permanently by infringing security measures, with the intention of gaining access, knowing such access is unauthorised	A fine not exceeding Kshs. 5 million or imprisonment for a term not exceeding 3 years, or both
Access with intent to commit further offence	Involves causing a computer system to perform a function temporarily or permanently by infringing security measures with the intention to commit other offences or to facilitate them	A fine not exceeding Ksh. 10 million shillings or imprisonment for a term not exceeding 10 years, or both
Unauthorized interference	Involves trespassing a computer system, program or data, intentionally and without authorisation/or consent of the person who is so entitled	A fine not exceeding Kshs. 10 million shillings or imprisonment for a term not exceeding 5 years, or both.

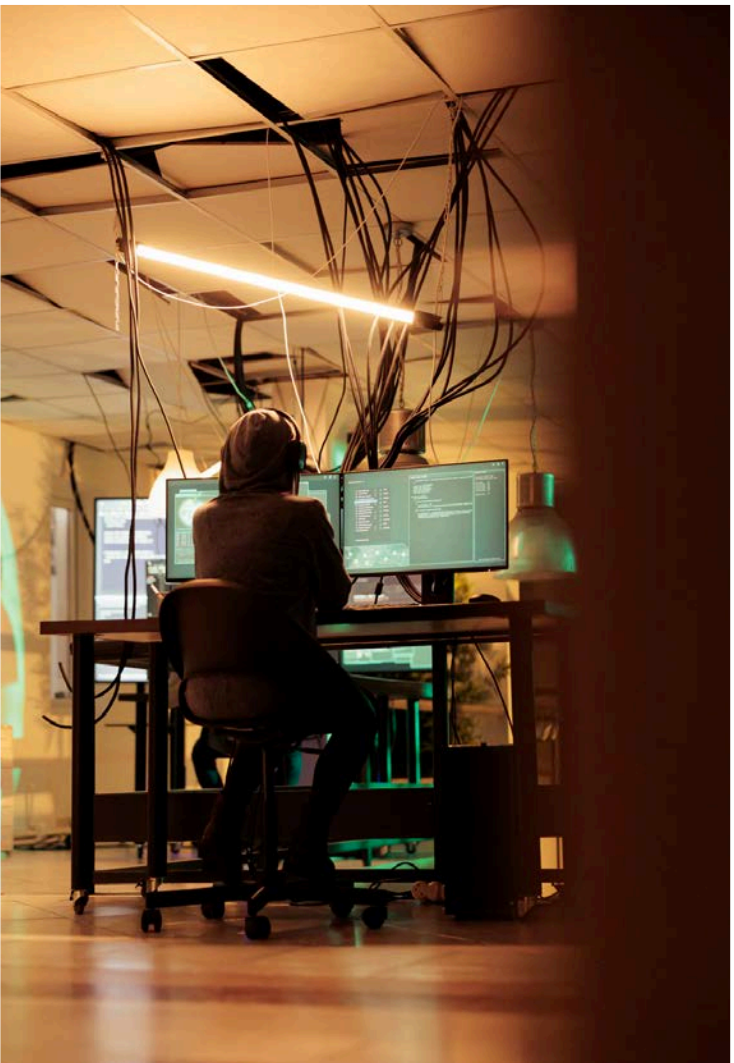
Offence	Description	Penalty
Unauthorized interception	Involves interrupting/blocking transmission of data to or from a computer system over a telecommunication system, intentionally and without authorisation, directly or indirectly	A fine not exceeding Kshs.10 million shillings or imprisonment for a term not exceeding 5 years, or both.
Illegal devices and access codes	Involves knowingly manufacturing, adapting, selling, procuring for use, importing, offering to supply, distribute or otherwise make available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence	A fine not exceeding Kshs. 10 million shillings or imprisonment for a term not exceeding 5 years, or both.
Unauthorised disclosure of password or access code	Involves disclosing any password, access code or other means of gaining access to any program or data held in any computer system knowingly and without authority	A fine not exceeding Kshs. 5 million shillings or imprisonment for a term not exceeding 3 years, or both.

Offence	Description	Penalty
Offences involving protected computer systems	Involved unauthorized access, interception, interference of protected computer system such as those that are necessary for security, defence or international relations, provision of services directly like communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically etc	A fine not exceeding Kshs. 25 million shillings or imprisonment for a term not exceeding 20 years or both.
Cyber espionage	Involves unlawfully and intentionally accessing or intercepting data, from or within a critical database or a national critical information infrastructure, with the intention of benefiting a foreign state against the Republic of Kenya directly or indirectly	A fine not exceeding Kshs. 10 million shillings or imprisonment for a period not exceeding 20 years, or both.
False Publication	Involves publishing false, misleading or fictitious data or misinforms with the intention that the data shall be considered or acted upon as authentic, with or without any financial gain	A fine not exceeding Kshs. 5 million shillings or imprisonment for a term not exceeding 2 years, or to both

Offence	Description	Penalty
Phishing	Involves creating or operating a website or sending a message through a computer system with the intention to inducing the user or the recipient to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system	A fine not exceeding Kshs. 300,000 or to imprisonment for a term not exceeding 3 years or both
Wrongful distribution of obscene or intimate images	Involves the transfer, publishing, or dissemination, including making a digital depiction available for distribution or downloading through telecommunications network or though any other means of transferring data to a computer, the intimate or obscene image of another person	A fine not exceeding Kshs. 200,000 or imprisonment for a term not exceeding 2 years, or both
Fraudulent use of electronic data	Involves causing any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer knowingly and without authority	A fine not exceeding Kshs. 200,000 or imprisonment for a term not exceeding 2 years, or both

Offence	Description	Penalty
Publication of false Information	Involves knowingly publishing information that is false, that is calculated or results in panic, chaos, violence among citizens, or which is likely to discredit the reputation of a person, on print, broadcast, data or over a computer system	A fine not exceeding Kshs. million shillings or imprisonment for a term not exceeding 10 years, or to both.
Child pornography	Involves intentionally producing, distributing, downloading, selling, possessing or publishing child pornography through a computer system	A fine not exceeding Kshs. 20 million or imprisonment for a term not exceeding 25 years, or both
Computer forgery	Involves intentionally inputting, altering, deleting, or suppressing computer data, resulting in inauthentic data, with the intent that it would be considered or acted upon as if it was authentic for legal purposes, regardless of whether the data is directly readable and intelligible or not	A fine not exceeding Kshs.10 million shillings or imprisonment for a term not exceeding 5 years, or both
Cyber terrorism	Involves accessing or causing to be accessed a computer or computer system or network for purposes of carrying out a terrorist act	A fine not exceeding Kshs. 5 million or imprisonment for a term not exceeding 10 years, or both

Offence	Description	Penalty
Computer fraud	Involves fraudulent or dishonest intention to unlawfully gain or obtain an economic benefit for oneself or for another person through unauthorised access to a computer system , program or data;	A fine not exceeding Kshs. 20 million shillings or imprisonment for a term not exceeding 10 years, or both
Cyber harassment	Involves willfully communicating directly or indirectly, to cause fear of violence, damage or loss on that a persons' property; or detrimentally affect that person	A fine not exceeding Kshs. 20 million shillings or imprisonment for a term not exceeding 10 years, or both
Cybersquatting	Involves intentionally taking or using 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	A fine not exceeding Kshs. 200,000 or imprisonment for a term not exceeding 2 years or both
Identity theft and impersonation	Identity theft and impersonation involves fraudulently or dishonestly using an electronic signature, a password, or any other unique identification feature of another person	A fine not exceeding Kshs. 200,000 or to imprisonment for a term not exceeding 3 years or both



Note: Under Section 46A, courts can take action against computer systems, websites, or digital devices used to promote unlawful activities such as terrorism, child sexual abuse content, religious extremism, or cultism.

Other Important Penalties Provided in the CMC Act include:

1. Confiscation of Property: Courts can take away money, property, or assets gained from cybercrime
2. Compensation for victims: Offenders may be ordered to pay victims for losses caused by the crime
3. Penalties for Companies: Companies involved in cybercrime can be fined heavily. Managers may also face jail time if they allow the offence

How are Offences Investigated under the CMC Act 2018?

Offense	Description
Search and seizure of stored computer data	• Police officers or authorized persons may apply to a court for a warrant to access, search, and seize computer data needed for criminal investigations or proceedings, or data obtained through an offence. • The warrant authorizes searches of specified persons or premises and remains valid until executed or cancelled. • Officers must present the warrant when carrying out the search, and anyone who obstructs the process, compromises data integrity or confidentiality, or misuses these powers commits an offence punishable by a fine of up to five million shillings, imprisonment of up to three years, or both.
Record of and access to seized data	• After a search or seizure of computer systems or data, the officer must record and list what was seized, including the date and time, and provide a copy to the affected person. • Individuals with lawful custody or rights to the data may request access or copies, unless this would risk an offence or harm an investigation or legal proceedings. In such cases, a court may still authorize access or copies if reasonable grounds are shown.
Production order	• Police officers or authorized persons may apply to a court for an order requiring a person to provide specific computer data or requiring a service provider in Kenya to provide relevant subscriber information needed for an investigation, where such data is in their possession or control.

Offense	Description
Expedited preservation and partial disclosure of traffic data	• Police officers or authorized persons may order the urgent preservation of specified traffic data needed for a criminal investigation where there is a risk it may be altered or lost, and may require limited disclosure to identify service providers and communication routes. • The data must be preserved confidentially for up to 30 days, with possible court-approved extensions, and service providers must promptly assist and disclose necessary non-content data to support the investigation.
Real-time collection of traffic data	• Police officers or authorized persons may apply to a court for an order allowing the real-time collection or recording of traffic data for a specific criminal investigation, including requiring service providers to assist within their technical capabilities. • The application must justify the need, identify the data, persons, and offences involved, and explain safeguards to protect third-party privacy. • Such orders may last up to six months and can be extended by the court if necessary, proportionate, and not overly burdensome, with confidentiality requirements imposed, and penalties for service providers who fail to comply.
Interception of content data	• Police officers or authorized persons may apply to a court for an order to intercept and collect the content of specified electronic communications in real time for a criminal investigation, including requiring service providers to assist within their technical capacity. • The application must justify the need, identify the data and offence, and explain privacy safeguards. • Such orders are time-limited to what is necessary, up to nine months with possible court-approved extensions, may be subject to confidentiality requirements, and non-compliance by service providers attracts significant fines or imprisonment.

What Sections of the CMCA 2018 have been changed by the CMC Amendment Act, 2025

CMCA 2018		CMCA AMENDMENT 2025
Focused on unauthorized access, data interference, cyberbullying, identity theft, and electronic fraud	Scope of offences	Expanded to include emerging technologies like AI misuse, deepfakes, and stricter rules on misinformation.
Fines up to 5 million KES and/or imprisonment depending on the offence	Penalties	Increased fines and longer jail terms for serious offences; some penalties updated to match modern cyber threats.
Basic provisions for protecting personal data in cyber offences.	Data Protection	Stronger data protection requirements and clearer regulations on data privacy.
Defined and penalized cyberbullying and online harassment	Cyberbullying & Harassment	Enhanced provisions targeting online harassment, including social media-specific rules.
Gives powers to investigate, arrest, and seize equipment related to cybercrimes.	Law Enforcement Powers	Broadened powers for authorities, including better cross-border cooperation and faster digital evidence handling.

CMCA 2018 vs CMCA AMENDMENT 2025

CMCA 2018		CMCA AMENDMENT 2025
Reporting mechanisms mainly through the Directorate of Criminal Investigations.	Offence Reporting	Introduced streamlined online reporting portals and victim support services.
Mainly traditional cybercrimes like hacking, phishing, and fraud.	Technology Focus	Addresses new tech threats like AI-generated content misuse, crypto crimes, and cyberterrorism.
Some measures for public education on cyber safety.	Public Awareness	Mandates ongoing national awareness campaigns and school programs on cyber hygiene.
Recognizes protection of children online but limited specific measures.	Focus on Children & Youth	Increased focus on protecting minors from cyber exploitation and abuse.

Contacts

Drop us a line
info@elgia.org

Give us a call
+254 (020) 367-3903

Office Location
CVS Plaza, Lenana Rd.

WITH SUPPORT FROM

Activity supported by the
Canada Fund for Local Initiatives

Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada