THE COMPUTER MISUSE AND CYBERCRIMES (CRITICAL INFORMATION INFRASTRUCTURE AND CYBERCRIME MANAGEMENT) REGULATIONS, 2023

ARRANGEMENT OF REGULATIONS

Regulation

THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018.

(No. 5 of 2018)

IN EXERCISE of the powers conferred by 70 of the Computer Misuse and Cybercrimes Act, 2018, the Cabinet Secretary for Interior and National Administration, makes the following Regulations—

THE COMPUTER MISUSE AND CYBERCRIMES (CRITICAL INFORMATION INFRASTRUCTURE AND CYBERCRIME MANAGEMENT) REGULATIONS, 2023

PART I— PRELIMINARY PROVISIONS

Citation.

1. These Regulations may be cited as the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2023.

Interpretation.

2. In these Regulations, unless the context otherwise requires —

No.5 of 2018.

"Act" means the Computer Misuse and Cybercrimes Act, 2018;

"accreditation certificate" means an accreditation certificate issued by government through the Root Certificate authority pursuant to these Regulations utilized for a wide range of e-transactions;

"authorized persons" has the meaning assigned under section 2 of the Act;

"auditor" means a person designated or appointed by the Committee to conduct an audit of a critical information infrastructure as provided under regulation 44;

"Cabinet Secretary" has the meaning assigned under section 2 of the Act;

"Chief Information Security Officer" means the person designated or appointed as a Chief Information Security Officer pursuant to regulation 33;

"Committee" has the meaning assigned under section 2 of the Act;

"critical data" includes any data, database, network, communications infrastructure;

"critical information infrastructure" includes critical information infrastructure system or data and national critical information infrastructure;

"Critical Information Infrastructure Cybersecurity Operations Centres" means the Cybersecurity Operations Centres established pursuant to these Regulations;

"critical information infrastructure system or data" has the meaning assigned under section 2 of the Act;

"cybersecurity incident" means any act or attempt, successful and unsuccessful, to gain unauthorised access to, disrupt or misuse a computer or computer system or information stored on the information system or critical information infrastructure which may have a disruptive effect that significantly impacts the following—

(a) the number of users relying on that service;
(b) the dependency of other sectors critical information infrastructure sectors on the service provided by that entity;

(c) the impact that incidents may have, in terms of degree and duration, on economic and societal activities or public safety;
(d) the market shares of the entity;
(e) the geographic spread regarding the area that may be affected by an incident; and
(f) the importance of the entity in maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

"cybersecurity service provider" means a service provider for the purpose of ensuring cybersecurity of the country or organization;

"designation" includes declaration of a critical information infrastructure by notice in the Kenya *Gazette* as contemplated under sections 11 and 13 of the Act;

"Director" means the Director of the National Computer and Cybercrimes Co-ordination Committee appointed under section 7 of the Act;

"emerging technologies" includes new technologies and the continuing development of existing technologies;

"establishment documents" include—
(a) a Statute, Charter or statutory instrument in which a body is established;
(b) registration certificate;
(c) trust deeds in which a trust has been established; or
(d) other instruments by which a body is established including its governing and administrative structure;

"financial year" means the period of twelve months ending on the thirtieth June each year;

"information infrastructure" means digital critical infrastructure;

"owner of critical information infrastructure" includes the operator, authorized person in control or any person in control of critical information infrastructure;

"National Cybersecurity Operations Centres" means the national focal point Cybersecurity Operations Centre established under regulation 10;

"premises" includes building and area surrounding the building in which a critical information infrastructure is situated;

"principle of least privilege (PoLP)" means an information security model which restricts access to the specific data, resources and applications required to undertake a task to a specific user or entity;

"Sector Cybersecurity Operations Centres" means the Cybersecurity Operations Centres established pursuant to regulation 11;

"Secretariat" means the Secretariat of the Committee established under section 7 of the Act;

"system" means the digital or physical infrastructure of a critical information infrastructure;

"third party" means in relation to cyber risks, external parties in the supply chain and who have access to organization's customer data, systems, processes, or other privileged information and may include: vendors, suppliers,

partners, contractors, or service providers, who have access to internal company or customer data, systems, processes, or other privileged information;

"transfer of a critical information infrastructure" includes copying or moving a program or data to—

(a) any computer system, device or storage medium other than that in which it is stored; or

(b) to a different location in the same computer system, device or storage medium in which it is stored;

(c) causing it to be output from the computer in which it is held, whether by having it displayed or in any other manner; or

(d) using it by causing the computer to execute a program or is itself a function of the program;

"vulnerabilities" means weaknesses or opportunities in a computer, computer system or critical information infrastructure, information system, security procedures, internal controls or implementation that may be exploited to gain unauthorized access or that may be exploited or triggered by a threat source.

Objects of the Regulations.

3. The object of these Regulations is to—

(a) provide a framework to monitor, detect and respond to cybersecurity threats in the cyberspace belonging to Kenya;
(b) provide for frameworks for establishment and management of Cybersecurity Operations Centres;

(c) provide for protection, preservation and management of critical information infrastructure;
(d) promote access to, transfer and control of data in any critical information infrastructure;
(e) provide for storage and archiving of critical data or information;
(f) provide for audit and inspection of national critical information infrastructure;
(g) provide for recovery plans in the event of a disaster, breach or loss of national critical information infrastructure or any part of it;
(h) provide a framework for capacity building on prevention, detection and mitigation of computer and cybercrimes and matters connected thereto as envisaged under section 6 (j) of the Act;
(i) promote coordination, collaboration, cooperation and shared responsibility amongst stakeholders in the cybersecurity sector including critical infrastructure protection;
(j) support integration and coordination of the functions of various stakeholders responsible for securing critical information infrastructure; and
(k) provide for mechanisms for cybercrime management.

Guiding principles.

4. The guiding principles under these Regulations shall be to promote—

(a) collaboration and coordination in cybercrime management and protection of critical information infrastructure amongst relevant stakeholders;
(b) public-private collaboration in the implementation of the Act and these Regulations;

(c) accountability, professionalism and responsibility in the use of information, communication and technology;
(d) digital trust, confidentiality, integrity, and availability of critical information infrastructure;
(e) minimization of the likelihood and impact of successful cyber-attacks;
(f) respect for rights of individuals including human dignity, equity and social justice; and
(g) good governance and integrity;
(h) trust.

Scope of Regulations.

5. (1) These Regulations shall apply to cybersecurity matters in the public sector and the private sector.

(2) Without prejudice to the generality of paragraph (1), these Regulations shall apply with respect to—

(a) the members of the public;
(b) to owners of critical information infrastructure; and
(c) cybersecurity service providers offering services as provided under the Act.

PART II—ADMINSTRATION AND MANAGEMENT OF THE COMMITTEE

Responsibilities of the Committee.

6. In addition to the functions of the Committee provided under section 6 (1) of the Act, the Committee shall—

(a) evaluate audit reports submitted by the Secretariat on designated critical information infrastructure;
(b) review the compliance reports submitted by the owners of the critical information infrastructure in accordance with section 13(1) of the Act;

(c) formulate codes of cybersecurity practice and standards of performance for owners of critical information infrastructure and sectors;
(d) issue prompt advice to Government on cybersecurity strategies relating to the application of blockchain technology, critical infrastructure, mobile money and trust accounts;
(e) undertake advocacy and create public awareness on cybersecurity matters;
(f) consider reports on emerging technologies and their impacts on security for informed decision making;
(g) approve the identification and designation of critical information infrastructure;
(h) receive and approve reports from the Cybersecurity Operations Centres;
(i) with respect to individual member of the Committee, attend and participate in the meetings of the Committee;
(j) approve the development and management of the National Public Key Infrastructure Frameworks;
(k) consider and approve non-financial and financial records submitted by the Director prior to submission to the Cabinet Secretary as provided under section 5(2) of the Act;
(l) co-ordinate cybersecurity research undertaken by the Secretariat and consider the research for informed decision making; and
(m) undertake any other responsibilities as the National Security Council or the Cabinet Secretary may direct.

Conduct of business of the Committee.

7. The conduct of business of the Committee shall be in the manner provided under the First Schedule of these Regulations.

Role of the Secretariat.

8. In addition to the functions of the Secretariat provided under section 7 (3) of the Act, the Secretariat shall—

(a) issue notices of meetings to the Committee members including organizing for the venue and time for the meetings;

(b) take minutes at meetings of the Committee and circulating draft minutes to all Committee members within seven working days from the date of such meetings;

(c) undertake auditing of designated critical information infrastructure in accordance with section 13(2) of the Act;

(d) provide prompt briefs to the Committee on all matters relating to National Cybersecurity Situation in the country for strategic decision making;

(e) maintain up-to date non-financial and financial records of the Committee and the Secretariat;

(f) facilitate the members of the Committee to enable them discharge their mandate;

(g) audit risk assessment reports by public bodies and private entities including owners of critical information infrastructure;

(h) maintain a database on critical information infrastructure;

(i) provide technical or non-technical support to Cybersecurity Operations Centres;

(j) prepare sector operational guidelines for effective implementation of the Act and these Regulations;

(k) conduct research on cybersecurity matters envisaged in the Act;

(l) keep and maintain a database on reported cyber threats and incidences including the action taken;

(m) prepare draft advisories or reports for consideration by the Committee;

(n) in consultation with the Committee, organize for information sharing with stakeholders;
(o) receive and analyses reports and prepare policy briefs for consideration by the Committee; and
(p) undertake any other duties assigned by the Committee for the effective discharge of the mandate of the Committee.

PART III— CYBERSECURITY OPERATIONS CENTRES

Division 1— Cybersecurity Operations Centres

Cybersecurity Operations Centres.

9. (1) In this Part, "Cybersecurity Operations Centres" includes—

(a) National Cybersecurity Operations Centre;
(b) Sector Cybersecurity Operations Centres; and
(c) Critical Information Infrastructure Cybersecurity Operations Centre.

(2) Pursuant section 6 (1) (f) and (g), the Committee shall coordinate the collection and analysis of cyber threats through collaboration and cooperation with the Cybersecurity Operations Centres.

(3) The Committee shall—

(a) report to the National Security Council on all cyber incidents reported by the Cybersecurity Operations Centres that threatens Kenya's cyberspace, as envisaged under section 6 (1) (f) of the Act;
(b) based on the reports received, advise the National Security Council on any matter relating to cybersecurity as provided under section 6 (1) (b) of the Act;
(c) provide guidance to Cybersecurity Operations Centres for the effective discharge of their respective mandate; and

(d) formulate code of cybersecurity practice and standards operating procedures for the Cybersecurity Operations Centres.

(4) The capability of a Cybersecurity Operations Centre shall include—

(a) cybersecurity specialists organized to prevent, detect, analyze and respond to threats;
(b) Threat prevention
(c) Threat monitoring and detection
(d) Incidence response
(e) Threat intelligence
(f) incident management.

National Cybersecurity Operations Centre.

10. (1) A National Cybersecurity Operations Centre shall be the national focal point for detection, monitoring, prohibition, prevention response and investigation of cyber threats, computer and cybercrimes on Cybersecurity in Kenya.

(2) Without prejudice to the generality of paragraph (1), the National Cybersecurity Operations Centre shall –

(a) have visibility of threats and incidents that occur in Sector Cybersecurity Operations Centre and Critical Information Infrastructure Cybersecurity Operations Centre;
(b) have the capability to perform the functions of a Sector Cybersecurity Operations Centre and Critical Information Infrastructure Cybersecurity Operations Centre;
(c) co-ordinate any cybersecurity incidents in the Sector Cybersecurity Operations Centre and Critical Information Infrastructure Cybersecurity Operations Centre including—
    (i) collection, analysis and response by the Cybersecurity Operations Centres;

(ii) having visibility of threats and incidents that occur in the Cybersecurity Operations Centre;
(iii) co-operating with computer incident response teams through sharing of threat intelligence to inform response to cyber incidents, utilizing technologies and tools;
(iv) receiving real-time information on cyber threats and incidents from the Cybersecurity Operations Centres;
(v) threat and information sharing;
(vi) joint exercises and training of the Cybersecurity Operations Centres; and
(vii) supporting supply chain risk management efforts.

(d) coordinate capacity building programs, research and development activities on cyber threats and incidents;

(e) report to the Committee on all cyber incidents reported by the Sector Cybersecurity Operations Centres and Critical Information Infrastructure Cybersecurity Operations Centres;

(f) convene cybersecurity fora through meetings, colloquiums, webinars, workshops or other consultative platforms for Cybersecurity Operations Centres in order to—
(i) facilitate consultations, co-ordination and collaboration in the implementation of relevant policies and laws;
(ii) make recommendations to the Committee aimed at improving Cybersecurity in the country;
(iii) promote data and information sharing including sharing of experiences, best

practices, on emerging issues on cybersecurity;

(iv) create awareness on cybersecurity;

(g) undertake research and development for tool engineering;

(h) facilitate co-Operations of the Committee with Sector Cybersecurity Operations Centres and Critical Information Infrastructure Cybersecurity Operations Centres and other relevant bodies, locally and internationally in response to threats of computer and cybercrime incidents;

(i) utilize threat intelligence from internal and external sources to enhance its situational awareness and response capabilities;

(j) facilitate the implementation of standards operating procedures formulated by the Committee to guide the Operations of the Cybersecurity Operations Centers;

(k) perform any other functions necessary for the confidentiality, integrity and availability of the Cybersecurity Operations Centers or as may be directed by the Committee.

Sector Cybersecurity Operations Centres.

11. (1) There shall be a Sector Cybersecurity Operations Centre which shall be responsible for detection, monitoring, prohibition, prevention response and investigation of cyber threats, computer and cybercrimes that are specific to their respective Sector.

(2) For the avoidance of doubt, a Sector Cybersecurity Operations Centre shall be—

(a) the Regulator of the specific Sector as set out in the Second Schedule in which the critical information infrastructure is domiciled; or

(b) where applicable, the relevant Ministry where the critical information infrastructure is domiciled.

(3) Without prejudice to the generality of paragraph (1), the Sector Cybersecurity Operations Centres shall –

(a) collaborate though information and threat intelligence sharing with the sector;

(b) coordinate advanced cyber threat analytics particularly on sector specific threats, incidence response, joint trainings or joint exercises and other cross-sectoral cybersecurity initiatives;

(c) have visibility of threats and incidents that occur in the Critical Information Infrastructure Cybersecurity Operations Centre in the Sector;

(d) have the requisite capability to perform the functions of a Sector Critical Information Infrastructure Cybersecurity Operations Centre;

(e) convene consultative fora through meetings, colloquiums, webinars, workshops or other platforms on sectoral issues of common interest to the sectors in order to—

(i) facilitate collaborations, consultations and co-ordination for the implementation of relevant policies and laws applicable in the Sector;

(ii) make recommendations to the sector aimed at improving cybersecurity at the Sector level;

(iii) promote data and information sharing within the sector including sharing of experiences, best practices, on emerging issues in the sector;

(iv) where applicable, implement the recommendations of the National cybersecurity Operations Centre; or

(v) build the capacity on cybersecurity in the sector;

(f) co-ordinate sectoral threat, monitoring and incidence response for Critical Information Infrastructure Cybersecurity Operations Centre in their respective Sector including—

(i) collection, analysis and response by the Critical Information Infrastructure Cybersecurity Operations Centres;

(ii) having visibility of threats and incidents that occur in the Critical Information Infrastructure Cybersecurity Operations Centre;

(iii) co-operating with computer incident response teams through sharing of threat intelligence to inform response to cyber incidents, utilizing technologies and tools;

(iv) receiving real-time information on cyber threats and incidents from the Critical Information Infrastructure Cybersecurity Operations Centres;

(v) threat and information sharing;

(vi) incidence response coordination;

(vii) joint exercises and training of the Critical Information Infrastructure Cybersecurity Operations Centres;

(viii) supporting supply chain risk management efforts.

(g) coordinate capacity building programs, research and development activities on cyber threats and incidents in the Sector;

(h) report to the National Cybersecurity Operations Centres on all cyber incidents reported by the Critical Information Infrastructure Cybersecurity Operations Centres in the Sector;

(i) undertake research and development for tool engineering;

(j) facilitate collaboration and cooperation amongst Critical Information Infrastructure Cybersecurity Operations Centres in the Sector;
(k) utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities;
(l) facilitate the implementation of standards operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centers; and
(m) perform any other function necessary for the confidentiality, integrity and availability of the Critical Information Infrastructure of their sectoral mandate.

(4) The administrative and other costs shall be borne by members of each Sector Cybersecurity Operations Centre.

Critical Information Infrastructure Cybersecurity Operations Centre.

12. (1) There shall be a Critical Information Infrastructure Cybersecurity Operations Centre which shall be responsible for detection, monitoring, prohibition, prevention, response and investigation of cyber threats, computer and cybercrimes for each owner of a Critical Information Infrastructure.

(2) Without prejudice to the generality of paragraph (1), the Critical Information Infrastructure Cybersecurity Operations Centre shall –

(a) collaborate with the relevant agencies, on cyberthreat surveillance and analysis;
(b) have the requisite capability to detect, monitor, prohibit, prevent, respond and investigate cyber threats, computer and cybercrimes at their respective organization;

(c) incidence detection, analysis and response in their respective Organization;
(d) undertake capacity building programs, research and development activities on cyber threats and incidents in the organization;
(e) report to the respective Sector Cybersecurity Operations Centres on all cyber incidents reported by their organization;
(f) undertake research and development for tool engineering;
(g) co-operate with other Critical Information Infrastructure Cybersecurity Operations Centres in their respective Sector;
(h) utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities;
(i) implement the codes or standard operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centers; or
(j) perform any other function as may be necessary for the confidentiality, integrity and availability of the Critical Information Infrastructure.

(3) Each organization shall meet the administrative costs and other expenses of their respective Critical Information Infrastructure Cybersecurity Operations Centre.

Capacity building by owners of critical information infrastructure.

13. (1) The owner of a critical information infrastructure shall establish and implement a cybersecurity awareness programme to educate and develop cybersecurity awareness for all persons who use, operate and manage the critical information infrastructure including to—

(a) promote awareness of relevant laws, regulations, codes of practice, policies, standards, guidelines and procedures;

(b) provide regular and timely communication covering general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations; and
(c) guide individual behavior and the security culture of the organization.

(2) The cybersecurity awareness programme under paragraph (1) shall include the following topics—
(a) cybersecurity;
(b) identification and reporting suspicious activity;
(c) incident management and response;
(d) insider threats;
(e) respective sector best practices;
(f) risk assessment including threat, vulnerability, consequence and mitigation; and
(g) best practices for physical security of the critical information infrastructure and other relevant areas on cybersecurity;
(h) Other relevant themes.

(3) The owner of critical information infrastructure shall in consultation with the Committee, review the cybersecurity awareness programme at least once every twelve months to ensure that the programme is adequate and that it remains up-to-date and relevant.

Outsourced capabilities.

14. (1) An owner of a critical information infrastructure including government owned critical information infrastructure who intends to outsource any Operations shall, in writing, notify the Committee prior to outsourcing.

(2) The owner of critical information infrastructure shall enter into an agreement with the external service provider agreement and shall ensure that the outsourced capabilities

do not disrupt the confidentiality, integrity and the availability of the critical information infrastructure.

(3) Despite paragraphs (1) and (2) the owner of a critical information infrastructure shall be held responsible for any outsourced capabilities.

(4) An agreement with an external service provider as contemplated under paragraph (2) shall where the service involves granting external service provider access to the database shall—

(a) assess, prior to entering an agreement with the external service provider, the cybersecurity risks involved in the engagement;

(b) expressly agree with the external service provider on the following, taking into account the risks contemplated under paragraph (a)—

(i) the data the external service provider may process and the permitted purposes of its use as required by the agreement between the parties;

(ii) the database systems that the external service provider may access;

(iii) the type of processing or activities the external service provider may perform;

(iv) the agreement duration, the manner of returning the data to the owner of critical information infrastructure at the end of the agreement, its destruction at the disposal of the external service provider and of reporting accordingly

to the owner of critical information infrastructure;

(v) the manner data security obligations which apply to the processor of the database according to these Regulations are implemented, and additional data security instructions set by the owner of critical information infrastructure, if any;

(vi) the external service provider shall have his authorized users sign an undertaking to protect the information confidentiality, to use the data only according to the agreement and to implement the data security measures prescribed in the agreement; and

(vii) where an owner of critical information infrastructure permitted the external service provider to provide the service through another entity, it shall be the duty of the owner of critical information infrastructure to include in the agreement with the other entity all the matters detailed in these Regulations.

(2) The external service provider shall report to the owner of the critical information infrastructure, at least quarterly, notifying on the status of implementation of their obligations under the agreement including notifying on any security incident.

Division II— Monitoring and Inspection for Cybersecurity Operations Centres.

Monthly briefs and compliance reports.

15. (1) The Cybersecurity Operations Centres established pursuant to these Regulations shall submit—

(a) monthly briefs of cybersecurity compliance status to the Committee through the Director; and
(b) annual compliance reports as envisaged under section 13(1) of the Act.

(2) The briefs and reports referred to under paragraph (1) shall include cyber risks, threats and incidents.

Monitoring and inspection of the safety of a Cybersecurity Operations Centres.

16. Subject to section 13 (3) of the Act, the Director shall periodically, monitor and inspect any Cybersecurity Operations Centres to ensure compliance with the Act and these Regulations.

Technical support to Cybersecurity Operations Centres.

17. Where there is an imminent threat in the nature of a cyber-attack that would amount to a computer and cybercrime to any Cybersecurity Operations Centres, the Director may on his own motion, or upon a request, inquire or provide the requisite technical or non-technical support to the Cybersecurity Operations Centre.

Risk assessment and evaluation of Cybersecurity Operations Centres.

18. (1) An owner of a critical information infrastructure shall, bi-annually conduct, a cyber-risk assessment and business impact analysis for all relevant activities including products, services, business functions and processes.

(2) Despite paragraph (1), every organization shall undertake a risk assessment within six months from the date of commencement of these Regulations.

(3) The cyber-risk assessment of an organization shall –
(a) identify potential internal and external threats including single points of failures that may cause disruption to critical activities;
(b) assess and prioritize potential risks and evaluate potential threats based on their operational impact and probability of their occurrence;

(c) select required controls to manage identified risks;
(d) define a treatment plan and implement business continuity management controls including –
    (i) information technology disaster recovery plan;
    (ii) crisis management plan;
    (iii)business continuity plan;
    (iv) cyber-incidences response plan; and
    (v) emergency response plan.
(e) evaluate the organization's security policies, procedures, codes of practice and the structuring of the security function;
(f) evaluate the methodology applied in management of the security procedures and the availability of tools to ensure security of the computer system and of the mode of utilizing the tools;
(g) undertake a technical analysis of the security of all components of the computer system by conducting system integrity tests to ensure system resistance to all kinds of dangers; and
(h) analyze and evaluate any dangers that may result from operating systems with any deficiencies discovered during the risk assessment exercise.

(4) The business impact analysis of an organization shall be based on—
(a) the potential impacts of business disruptions for each prioritized business function and processes including financial, operational, customer, legal and regulatory impacts;
(b) recovery time objectives, recovery point objectives and maximum acceptable outage;
(c) internal and external inter-dependencies; and
(d) the resources required for recovery.

(5) An organization shall, at the conclusion of the risk assessment exercise, submit a risk register to the Committee through the Director.

(6) The risk register under paragraph (4) shall contain—

(a) a description and complete evaluation of the security of the computer systems of the organization or critical information infrastructure;
(b) the implementation of the treatment plan and adopted measures proposed in the preceding risk assessment, if any, and the deficiencies observed in the implementation of recommendations;
(c) a detailed analysis of the organization's technical deficiencies regarding the security procedures and tools adopted including an evaluation of the risks that may result from operating with the deficiencies discovered; and
(d) proposed organizational and technical security solutions to be adopted in order to overcome the shortcomings noted.

(7) The Director may, upon evaluating the risk register, request the organization to provide the Director with further information, and may carry out an inspection of the institution for the purposes of verification of the matters relating to the risk assessment.

(8) The Director may reject a risk register where—

(a) the risk assessment is carried out in contravention of the Act and these Regulations or any other stipulated procedures; or

(b) the risk register does not contain material information regarding the deficiencies identified by the exercise.

PART IV—CRITICAL INFORMATION INFRASTRUCTURE

Division I— Critical Information Infrastructure

Designation of critical infrastructure.

19. (1) Pursuant to section 9 of the Act, the Director shall in designating a system as a critical infrastructure —

(a) identify the system being designated as a critical information infrastructure;
(b) identify the owner of a critical information infrastructure;
(c) inform the owner of critical information infrastructure of his responsibilities under the Act and these Regulations;
(d) provide the owner of critical information infrastructure with particulars of the requirement to designate a chief information security officer to provide the requisite technical support to the organization; and
(e) any other matter that the Director may deem fit.

(2) The Director shall designate a critical information infrastructure in the manner specified in the Second Schedule.

(3) The following criteria shall guide the classification of a critical information infrastructure –

(a) sensitivity of the critical information infrastructure including sensitive (ICT based sector) critical information infrastructure or non-sensitive critical information infrastructure;

(b) the critical sector including transport, energy or health;
(c) the critical sub-sector including aviation, petroleum, pharmaceuticals;
(d) the critical services including food supply, distribution, banking, transport network (rail, road and air) or epidemic control; or
(e) interdependency within critical sectors, cross-sector relations and intra-sector relations, in which the critical information infrastructure is domiciled.

(4) Subject to paragraph (5), the details of information specified under paragraphs (1) and (2) shall be published in the *Gazette* notice contemplated under section 9(1) of the Act.

(5) The publication of designated critical information infrastructure in the Kenya *Gazette* as contemplated under section 9 (1) of the Act shall not include exempt information envisaged under section 6 of the Access to Information Act, 2016.

No. 31 of 2016.

Notice to owner on designation.

20. (1) The Director shall, within seven days of designating a critical information infrastructure, inform the owner in writing as contemplated under section 9 (3) of the Act.

(2) The notice to the owner under paragraph (1), shall give reasons for the designation of the system as a critical information infrastructure.

Directives upon designation.

21. (1) The Director shall, within seven days, upon notifying the owner of critical information infrastructure, issue directives contemplated under section 9(4) of the Act to the owner of critical information infrastructure.

(2) Without prejudice to the generality of paragraph (1) and in addition to the directives specified under section 9(4) of the Act, the Director may direct the owner critical information infrastructure to—

(a) conduct regular risk assessment;
(b) develop incidence response plans;
(c) implement suitable security measures including firewalls and access controls; or
(d) ensure personnel are adequately trained in security best practices.

Failure to implement directives.

22. (1) The Director shall upon expiry of the timelines given to the owner of critical information infrastructure to implement the Directives issued under regulation 21 issue a notice to show cause to the owner of critical information infrastructure.

(2) Where the Director upon providing the owner of critical information infrastructure with the opportunity to be heard in accordance with the Fair Administrative Action Act, 2015, and where applicable order for suitable actions or administrative sanctions to be imposed against the owner of critical information infrastructure.

No. 4 of 2015.

(3) The suitable actions or administrative actions contemplated under paragraph (1) may include orders to—

(a) provide a detailed report on non-compliance to the National Security Council;
(b) inform the respective Regulator to impose specified actions under their respective law;
(c) be under twenty-four hours' surveillance by the Director;
(d) constitute a multi-agency committee to implement the directives;
(e) fully implement the directives by the Director;
(f) require investigations by the law enforcement agencies; or

(g) where necessary, refer the matter to the Office of the Director of Public Prosecutions.

(4) Where an owner of critical information infrastructure is aggrieved by the decision of the Director, he may appeal to the Committee.

Gazettement by the Committee of critical information infrastructure.

23. (1) Pursuant to section 10 of the Act—

(a) the Committee shall, in consultation with the owner of a critical information infrastructure, and within seven days of identifying a critical information infrastructure submit its recommendations for Gazettement to the National Security Council; or

(b) the owner may apply to the Committee for Gazettement of their critical infrastructure using the process outlined under regulation 24.

(2) In identifying the critical information infrastructure, the Committee shall be guided by the criteria set out under section 9 (2) of the Act.

(3) Regulations 19, 20, 21 and 22 shall, with necessary modifications, apply to this regulation.

Application by owner of critical information infrastructure.

24. (1) An owner of a critical information infrastructure may, in writing, apply, to the Director for declaration of a system as a critical information infrastructure in accordance with the Act and these Regulations.

(2) The application under paragraph (1) shall—

(a) be in Form CMCA 1 set out in the Third Schedule;

(b) provide particulars of the owner of the critical information infrastructure which may include—
    (i) a copy of the establishment documents;
    (ii) particulars of the operators of the critical information infrastructure including name and contact details;
    (iii) a description of the sector under which the critical information infrastructure operates;
    (iv) a description of the services provided by the critical information infrastructure; and
    (v) a description of a third-party having access to the critical information infrastructure.
(c) specify the sector in which the system is domiciled;
(d) detail the resources available to the owner or person in control of the system to—
(e) safeguard the system against destruction, disruption, failure or degradation;
(f) repair or replace the system, including the critical infrastructure's equipment, materials or service; or
(g) recover the system from any destruction, disruption, failure or degradation; and
(h) detail the effects or the risk of a destruction, disruption, failure or degradation of the system on—

    (i) life;
    (ii) economy;
    (iii) public health and safety;

(iv) money markets of the Republic; and

(v) security,

in accordance with section 9(2) of the Act.

Consideration of application for declaration of critical information infrastructure.

25. (1) Upon receiving an application for declaration of a system as critical information infrastructure under section 24 of the Act, the Director shall—

(a) be guided by the criteria referred to under section 9 (2) of the Act in order to determine whether the system qualifies for designation as a critical information infrastructure;

(b) evaluate the potential risk of the system, taking into account—

(i) the probability of failure, disruption or destruction of the system in question or threat thereof; and

(ii) the impact and consequence of failure, disruption or destruction of infrastructure or threat thereof; and

(iii) consider the extent to which the designation as critical information infrastructure shall promote public interests.

(3) Where the Director is satisfied that the system has met the criteria for designation as a critical infrastructure, the Director shall—

(a) within seven days by notice in the *Gazette* designate the system as a critical information infrastructure; and

(b) notify the applicant, in writing, of the designation.

(4) Where the Director declines the application for designating a system as a critical information infrastructure,

the Director shall, in writing, notify the applicant within fourteen days.

(5) Where an applicant is aggrieved by the decision under paragraph (4), the applicant may apply the provision of regulation 73 on dispute resolution.

Register of critical information infrastructure.

26. (1) The Director shall keep and maintain an up-to-date Register of the critical information infrastructure designated under the Act and these Regulations.

(2) An owner of a critical information infrastructure shall furnish the Director of a critical information infrastructure within twenty-one days from the date of designation of the critical information infrastructure any additional particulars or any change in material particulars of the critical information infrastructure to the Director.

Changes to critical information infrastructure.

27. (1) An owner of a critical information infrastructure shall not make any significant change to the design, configuration, security or Operations of a critical information infrastructure, without prior approval of the Director.

(2) An owner of a critical information infrastructure who intends to make any change in the design, configuration, security or Operations of a critical information infrastructure shall thirty days before implementing the proposed changes apply in Form CMCA 2 set out in the Third Schedule to the Director specifying the reason for the changes to the critical information infrastructure.

(3) The Director shall consider the application within forty-eight hours and may approve or decline the application and in considering the application consider the following—

(a) evaluated implications of the proposed changed to the Operations, personnel, and

infrastructure of the critical information infrastructure;

(b) whether there would be any requirement for additional directives from the Committee to safeguard the security, confidentiality and integrity of the critical information infrastructure; or

(c) any other consideration that the Committee may deem necessary.

(4) The Director shall communicate the decision on approval or refusal to approve an application under this regulation to the owner of a critical information infrastructure within seven days giving reasons in case of a refusal.

(5) Any person who contravenes the provisions of this regulation commits an offence chargeable under section 14 (2) (b), (c) and (d) of the Act.

Change of ownership.

28. (1) Where there is a change in the ownership of an owner of a critical information infrastructure, the owner of a critical information infrastructure shall within seven days prior to the change notify the Director in Form CMCA 2 set in the Third Schedule.

(2) For the avoidance of doubt, the owner of a critical information infrastructure shall provide the particulars specified under regulation 24 and 25.

(3) In circumstances where the new owner of a critical information infrastructure seeks to undertake a lawful activity which may impact on the confidentiality, integrity and availability of critical information infrastructure or its associated dependent assets and systems, the owner shall make a written request for approval by the Committee.

(4) Any person who contravenes the provisions of this section commits an offence chargeable under section 14 of the Act.

Localisation of critical information.

29. (1) An owner of a critical information infrastructure shall ensure that the infrastructure on which critical information is domiciled is located in Kenya.

(2) An owner of a critical information infrastructure who intends to have critical information located outside Kenya, shall apply to the Committee in Form CMCA 3 set out in the Third Schedule.

(3) The Committee shall consider the application and may approve or decline to approve the application under paragraph (2), and shall communicate its decision within thirty days of receipt of the application.

(4) The Committee may, in considering an application by the operator to have critical information located outside Kenya take into account—

(a) security measures and safeguards being applied to the information and infrastructure on which the information is contained are adequate;
(b) whether it is necessary for the information to be stored outside the geographical jurisdiction of the Republic;
(c) national security;
(d) public interest;
(e) security of data including personal data contained in the critical information infrastructure;
(f) submissions by concerned operator; and
(g) any other factors that the Director considers necessary.

(5) The Committee shall consult the National Security Council and the relevant security agencies, when considering an application by the owner of a critical information infrastructure to have critical information located outside Kenya.

(6) Where the Director declines to approve the application under this regulation, the Director shall notify the operator within seven days of making such a decision.

Division II— Protection, Preservation and Management of Critical Information Infrastructure

Obligations of owners.

30. (1) Upon receipt of the notice and directives under regulations 20 and 21, the owner of a critical information infrastructure shall implement the directives within the time specified in the notice issued by the Director.

(2) An owner of a critical information infrastructure shall implement effective measures for ensuring—

(a) the physical security of the hardware and other critical infrastructure where the critical information infrastructure system is located;
(b) limitation of access to the critical information infrastructure or information stored in the critical information infrastructure;
(c) periodic maintenance and security testing;
(d) facilitate prompt access to the critical information infrastructure by authorized persons;
(e) administrative control of personnel having access to various components of the critical information infrastructure;
(f) limitations on use of removable storage devices;

(g) preparedness against damage or unauthorized access plans in the event of a disaster, breach or loss of a critical information infrastructure;
(h) undertake risk assessment identifying risk based security factors necessary to protect public health and safety, or national socio-economic security, where applicable;
(i) utilize innovative methods available in the market of securing the critical information infrastructure against cyberattack; or
(j) any other directives that the Director may from time to time issue.

(2) The owner of a critical information infrastructure may request, in writing, any support from the Director, which may be necessary for the effective implementation of the directives.

Baseline security for critical information infrastructure.

31. Every designated owner of critical information infrastructure shall adhere to the following baseline security requirements to ensure the protection of the critical information infrastructure—

(a) develop and implement an internal Cybersecurity Policy addressing the critical information infrastructure risks, consistent with the provisions of the Act and these Regulations and best practices relevant to the relevant sector and which shall—
(i) be reviewed at least annually, consistent with identified risks and threats affecting the specific critical information infrastructure sector;
(ii) addresses data protection concerns of the designated critical information infrastructure owner, consistent with the

No, 24 of 2019.

provisions of the Data Protection Act, 2019;

(b) implement and comply with the directives issued under regulation 21; and

(c) appoint or designate a Chief Information Security Officer in accordance with the requirements of regulation 33.

(2) The owner of a critical information infrastructure shall adopt the following technical and organizational measures for the protection of the designated critical information infrastructure—

(a) identifying, classifying and cataloguing all critical information infrastructure assets;

(b) controlling and managing access to critical information infrastructure systems and services.

(c) implementing the relevant security measures to mitigate cyber risk posed by employees, customers, suppliers, service providers, and other third-party affiliates;

(d) conducting security screening on all personnel handling critical information infrastructure information or data in the designated critical information infrastructure;

(e) conducting appropriate level of information and cybersecurity awareness and training for all employees of the designated critical information infrastructure Owner;

(f) implementing appropriate security monitoring and response process for timely detection of cybersecurity incidents targeting the designated critical information infrastructure;

(g) implementing relevant physical security measures for the physical protection of critical information infrastructure systems and its associated dependent assets and systems;

(h) implementing relevant infrastructure and cybersecurity measures to mitigate equipment failure including maintenance and software updates;
(i) developing, periodic test and updating business continuity and disaster recovery plan to ensure adequacy of such plans to support incident response and security redundancy operations;
(j) conducting a bi-annual cybersecurity risk assessment to identify existing vulnerabilities to which the designated critical information infrastructure is exposed as contemplated by regulation 18;
(k) conducting annual cybersecurity internal audits to check compliance with the directives under regulation 21;
(l) creating and maintaining a cybersecurity risk register with catalogues and profiling the various information and cyber risks targeted at the designated critical information infrastructure;
(m) conducting and participating in cybersecurity activities in collaboration with the Committee and other critical information infrastructure sectors for the purposes of testing the state of readiness of designated critical information infrastructure in responding to cybersecurity incidents;
(n) adopting relevant cybersecurity best practices, frameworks, and standards approved by the Committee; and
(o) ensuring that public key and source codes of critical information infrastructure systems are kept in escrow.

Incidence reporting for a critical information infrastructure.

32. In the event of a cybersecurity incident, the owner of a critical information infrastructure shall—

(a) facilitate the investigations by law enforcement agencies;

(b) report and mitigate impact of the incident in accordance with the cybersecurity standards formulated by the Committee;
(c) report all cybersecurity incidents to the relevant Sectoral Cybersecurity Operations Centres within twenty-four hours of becoming aware of an incident pursuant to section 40 of Act;
(d) establishing a point of contact such as the Chief Information Security Officer for reporting cybersecurity incidents and receiving cybersecurity information, including security advisories relevant to the particular designated critical information infrastructure sector;
(e) disclosing and reporting any vulnerabilities identified or discovered through internal or external security audits and assessments, within seventy-two hours of identifying or discovering the vulnerability.

Designation of the Chief Information Security Officer.

33. (1) An owner of critical information infrastructure may designate or appoint a Chief Information Security Officer on such terms and conditions as the owner may determine.

(2) Without prejudice to paragraph (1), a group of owners of critical information infrastructure may appoint a single Chief Information Security Officer, provided that the officer is accessible by each owner.

(3) The Chief Information Security Officer shall, amongst other duties, be—

(a) responsible for –

(i) cybersecurity matters in the organization in which the

critical information infrastructure is domiciled;

(ii) developing, implementing, and enforcing security policies to protect critical information infrastructure;

(iii) analyzing information technology security threats in real-time and mitigating the threats;

(iv) ensuring that newly-acquired technology complies with the cybersecurity standards;

(v) collaborating with the National Cybersecurity Operations Centres, Sector Cybersecurity Operations Centres and other relevant stakeholder to determine possible risks and risk management processes;

(vi) advising the owner of a critical information infrastructure;

(vii) creating cybersecurity awareness amongst members of staff and users;

(viii) assists in detection, identification, prevention, response, and recovery measures for cyber threats, risks or incidence in the organization;

(ix) ensuring compliance of the organization with the requirements of the Act and these Regulations; and

(b) the point of contact for the cybersecurity matters for the organization.

Mandatory requirements.

34. (1) An owner of a critical information infrastructure shall within six months from the date of commencement of these Regulations, formulate organizational policies, procedures and codes of practice for protection, preservation and management of the critical information infrastructure.

(2) Without prejudice to the generality of paragraph (1), the owner of a critical information infrastructure shall in the instruments specified under paragraph (1) specify—

(a) the storage and archiving modalities;
(b) sharing of critical information infrastructure system or data within the organization;
(c) transfer of critical information infrastructure system or data to third parties; and
(d) collection, use, storage, retention, deleting, correction, transfer or sharing of critical information infrastructure system or data

(3) The owner of a critical information infrastructure may implement cybersecurity requirements relating to projects, software and their application on a critical information infrastructure, which may include—

(a) using secure coding standards;
(b) using trusted and licensed sources for software development tools and libraries;
(c) conducting compliance test for software against the defined organizational cybersecurity requirements;
(d) secure integration between software components; or

(e) conducting a configurations' review, secure configuration and hardening and patching before going live for software products.

(3) Where an owner intends to change the management (change management or material change) of a critical information infrastructure projects, software and their application change management shall undertake—

(a) vulnerability assessment and remediation; and

(b) conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.

Mandatory requirements for gateways.

35. (1) The owner or operator of a gateway shall—

(a) maintain minimum cybersecurity standards as specified by the Committee to ensure their integrity, confidentiality and availability;

(b) implement access control mechanisms for gateways, for access only by authorized personnel;

(c) report any security incidents or breaches as provided under regulation 32;

(d) establish procedures for responding to and mitigating cyber incidents to prevent further damage;

(e) undertake periodic security audits conducted by independent third-party entities in order to—

(i) assess the gateway's security posture; and

(ii) ensure compliance with established standards and identify vulnerabilities;

(f) utilize secure communication protocols and encryption for data transmission through

gateways, in order to reduce the risk of data interception and manipulation;

(g) promote transparency in disclosure of known vulnerabilities and quick patches; and

(h) ensuring adequate cybersecurity measures by gateway vendors providing products or services including regular security updates.

(2) A owner, operator or vendor of a gateway who contravenes paragraph (1) commits an offence chargeable under section 20 of the Act.

Integration of critical information infrastructure.

36. (1) An operator of critical information infrastructure shall integrate or permit the integration of the critical information infrastructure with any other information infrastructure where such integration has met proper safety standards including safeguards specified under paragraph (2).

(2) In evaluating the adequate safeguards or measures of a third-party information infrastructure, the Director shall ensure that—

(a) the security of the critical information infrastructure is not compromised;

(b) the third-party information infrastructure has adequate safeguards or measures; and

(c) access to the critical information infrastructure is in accordance with standards issued by the Committee.

Protection and preservation of premises and surrounding areas.

37. (1) An owner of critical information infrastructure shall implement appropriate safeguards and measures to ensure security of the premises and surrounding area in which a critical information infrastructure is situated.

(2) Without prejudice to the generality of paragraph (1), security measures on a premises in which a critical information infrastructure is situated may include—

(a) systems are maintained in a secure place, preventing unauthorized access, and which is suitable to the nature of the database activity and the sensitivity of information therein;
(b) where applicable, sufficient cooling mechanisms to prevent overheating of equipment;
(c) equipment to prevent or mitigate the effect of a fluctuation of an electric load;
(d) take measures to monitor and document the entry to and exit from sites in which the database or database systems are located, including the setting and removing of equipment in and from the database systems;
(e) ensure that critical information infrastructure is not used for general storage of any material that is not connected to the Operations or maintenance of the database;
(f) secure the area surrounding the premises or space in which a critical information infrastructure is domiciled; and
(g) any other measures necessary to maintain the confidentiality integrity and availability of the critical information infrastructure.

Access to critical information infrastructure.

38. (1) An owner of a critical information infrastructure shall develop a system of security clearance levels for personnel and third parties to access a critical information infrastructure.

(2) An owner of a critical information infrastructure shall restrict and ensure adequate measures are in place to monitor permitted access to a critical information infrastructure system or data.

(3) Without prejudice to the generality of paragraph (2), the measures contemplated under paragraph (2) may include —

(a) taking lawful steps as may be necessary, to secure a critical information infrastructure and the personnel or third parties present at the critical infrastructure;
(b) issuing, in writing, procedures for permitting entry to a critical information infrastructure;
(c) ensuring that a notice on permitted entry is displayed in a conspicuous manner at the entrance to the critical information infrastructure;
(d) providing proper visitor management system or record keeping system providing for details on identification, registration, escorting and monitoring of personnel, third parties or any visitor to the premises;
(e) providing mechanisms to protect critical information infrastructure systems from any disaster including use of firefighting system and proper climate control equipment;
(f) installing surveillance cameras at the proper location to monitor the movements and activities within areas hosting a critical information infrastructure;
(g) formulating its organizational Operational guidelines to guide the personnel, third parties on the manner in which the critical information infrastructure shall be accessed whether physically or virtually; and
(h) undertaking any action necessary to restrict access to a critical information infrastructure.

(4) In granting permission to access a critical information infrastructure, a person shall —

(a) furnish proof of their identity including contact details and any other relevant information required by the owner of a critical information infrastructure;
(b) declare possession of any item, object or thing that would be dangerous to the safety of the critical information infrastructure;
(c) declare the contents of any vehicle, suitcase, bag, handbag, folder, envelope, parcel or container of any nature, which is in the possession, custody or control of the person; and
(d) subject himself and anything in his possession or under his control to an examination by an electronic or other apparatus, for purposes of determining possession of any dangerous or prohibited item, thing or object.

(5) Upon granting access to a critical information infrastructure, the owner shall require the person to comply with the conditions including—

(a) carrying or displaying of the proof of permitted access;
(b) restriction of access to certain parts of the critical infrastructure including restricted access to the personnel within the critical information infrastructure;
(c) duration of access to the critical information infrastructure;
(d) monitored access including being escorted while on or in the critical information infrastructure; and
(e) other conditions as the owner of a critical information infrastructure may impose.

(6) An owner of a critical information infrastructure may, at any time, remove any person who has been granted access under this regulation, if—

(a) it is found that the access was unauthorized;

(b) the person is in breach, refuses or fails to comply with any conditions for access to the critical information infrastructure; or

(c) it is necessary for the securing of the critical infrastructure, contents of the critical information infrastructure including the personnel.

(7) An owner of a critical information infrastructure shall, where there is a violation of any of the requirements on access to a critical information infrastructure specified under the Act or these Regulations, inform the relevant government institution to investigate or prosecute a person on any offence specified under Part III of the Act.

Virtual access to critical information infrastructure.

39. (1) Regulation 38 shall, with necessary modifications, apply to any person who seeks virtual access to a critical information infrastructure.

(2) In addition, the owner of a critical information infrastructure shall—

(a) apply the principle of least privilege (PoLP) in granting access to critical information infrastructure systems;

(b) implement security logging and monitoring system to capture logs from critical information infrastructure system and periodically analyze the logs to ensure integrity of the critical information infrastructure system including detection of cybersecurity threats, risks or unauthorized access;

(c) install intrusion detection and prevention systems in order to monitor network traffic,

detect potential intrusions, and prevent unauthorized access; and

(d) adopt procedures for conducting regular security audits and penetration testing to identify vulnerabilities and system weaknesses.

Register of persons accessing critical information infrastructure.

40. (1) An owner of a critical information infrastructure shall keep and maintain an up-to-date register of persons having access to a critical information infrastructure.

(2) The register contemplated under paragraph (1) shall specify—

(a) the identification particulars of the person granted access to a critical information infrastructure including nationality;

(b) reason for accessing the critical information infrastructure;

(c) the extent of the authorization and restrictions applicable relating to accessing the critical information infrastructure;

(d) the duration of access to the critical information infrastructure;

(e) any archived data on the critical information infrastructure system or data; and

(f) any other requirements that the owner of a critical information infrastructure may from time to time determine.

(3) The Director, may request the owner of a critical information infrastructure to periodically or at any time as may be necessary, —

(a) examine the register, where there is a disruption or potential disruption of the system or any other circumstances that seeks to compromise the integrity of the critical information infrastructure; or

(b) request for extracts of the register,

for purposes of auditing compliance with any directives issued under the Act and these Regulations.

Storage and archiving of critical data or information.

41. (1) An owner of a critical information infrastructure may, where critical information infrastructure system or data is no longer immediately required for use, place the information in an archive for storage purposes.

(2) Where critical information infrastructure system or data has been stored in an archive, the adequate security standards, policies, procedures and codes of practice that apply to critical information infrastructure under these Regulations and the Act, shall apply to archived critical information infrastructure system or data.

Disaster recovery of critical information infrastructure.

42. (1) An owner of a critical information infrastructure shall establish a disaster recovery and backup site which may be independent of each other and shall be independent from the location of the critical information infrastructure.

(2) The owner of critical information infrastructure shall—

(a) be stored in a format that permits the retrieval of the information and restoration of an infrastructure in the event of a compromise or destruction of the infrastructure;

(b) retain the backup copy of the data in the system and establish security procedures in a manner that ensures the integrity of the critical information and the ability to restore the information in case of loss or destruction;

(c) establish procedures for routine periodical backup in accordance with these Regulations;

(d) formulate internal procedures to ensure restoration of the critical information in case of a disaster; and
(e) document security incidents pursuant to regulation 32, including the process of restoring the critical information, the identity of the personnel or third party involved in the restoration of the critical information and the details of the information restored.

Transfer of critical. information infrastructure.

43. (1) An owner of a critical information infrastructure shall not, without written authorization of the Director transfer fully, or partially any component of the critical information infrastructure.

(2) An owner of a critical information infrastructure who contravenes paragraph (1) commits an offence chargeable under section 20 of the Act.

Division III— Auditing and Inspection of Critical Information Infrastructure

Requirements for an auditor.

44. (1) The Director shall appoint such number of auditors as may be necessary, who shall be responsible for carrying out audit of a critical information infrastructure in the manner provided under section 13 of the Act.

(2) A person shall be qualified to be appointed as an auditor for a critical information infrastructure, if that person—
(a) is a citizen of Kenya;
(b) has at least a degree from a university recognized in Kenya;
(c) a cybersecurity expert with auditing qualifications from a recognized professional body of knowledge;
(d) a member in good standing of a cybersecurity professional body recognized in Kenya;

(e) has at least ten years' professional experience of conducting audits of critical information infrastructure;
(f) has demonstrable technical skills, competencies and knowledge on critical information infrastructure audit;
(g) satisfies the requirements of Chapter Six of the Constitution; and
(h) meets any other qualification which the Director may consider appropriate.

(3) The person appointed as an auditor of a critical information infrastructure under paragraph (1) shall be deemed to be a staff of the Committee.

(4) Upon being appointed, the Director shall issue the auditor with an appointment certificate in Form CMCA 4 set out in the Third Schedule.

(5) The auditor shall be required to carry and produce the certificate of appointment to the owner of a critical information infrastructure when carrying out an audit exercise.

Powers of auditor.

45. An auditor shall have all powers necessary for the effective discharge of his mandate, including powers to –

(a) upon giving notice to the owner as contemplated under section 13(2) of the Act, enter a premises to monitor and evaluate the compliance with the directives issues pursuant to these Regulations;
(b) require the production of any documents, additional information or any other matter which would assist in carrying out the audit;
(c) any other powers necessary to carry out the audit of a critical information infrastructure.

Compliance report by owner of critical information infrastructure.

46. (1) Pursuant to section 13 (1) of the Act, the owner of a critical information infrastructure shall within three months after the end of each financial year, submit to the Director a compliance report in line with the critical infrastructure framework demonstrating compliance with the framework.

(2) Without prejudice to the generality of paragraph (1), the compliance report shall amongst other things—

(a) demonstrate compliance with the critical infrastructure framework;
(b) verify compliance with the requirements of the Act and these Regulations;
(c) assess the adequacy and effectiveness of safeguards and measures put in place by the owner of a critical information infrastructure to meet the requirements of the Act and the Regulations;
(d) assess whether the owner of a critical information infrastructure has in place and implements the organizational policies, standards and procedure on cyber security; and
(e) identify risks and mitigation measure on a critical information infrastructure.

(3) The compliance report submitted to the Director under this regulation shall contain—

(a) risk assessment specifying the risks a critical information infrastructure is prone to and the mitigation measures the owner of a critical information infrastructure may apply; and
(b) the risk register by the critical information infrastructure.

(4) The Director shall within seven days of receipt of the compliance report submit it to the Committee.

(5) Upon consideration of the compliance report under paragraph (3), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the Committee.

(6) The recommendations by the Committee shall form the subject of evaluation by the auditor in the subsequent audit exercise.

(7) The Committee shall submit its reports to the National Security Council.

Requirement for audit.

47. (1) The Director shall conduct an annual audit or at any time where there is an imminent threat in the nature of an attack that amounts to an attack to a computer or cybercrime as contemplated under section 13 (2) of the Act.

(2) The Director shall notify an owner of a critical information infrastructure in Form CMCA 5 set out in the Third Schedule of –

(a) the date and time in which the audit shall be carried out;
(b) the identification particulars of the auditor;
(c) requirement for the owner of the critical information infrastructure to furnish the Director with the staff or contact person in the organization responsible for the overall management and control of the critical information infrastructure audit;
(d) specific documents required to be furnished to the auditor, prior to or during the audit exercise;
(e) furnish the owner of a critical information infrastructure with particulars of auditor prior to the date of commencement of the audit exercise;
(f) any other details relevant for the effective discharge of the audit.

Audit approach.

48. (1) The audit undertaken under these Regulations shall adopt both a compliance and risk-based approach.

(2) The compliance based audit approach shall carry out compliance test to ascertain the adequacy and effectiveness of the controls applied in the critical information infrastructure to comply with the Act and these Regulations.

(3) The risk-based audit approach shall identify the risks and threats that the critical information infrastructure is susceptible to and ascertain if established controls are appropriate to mitigate the identified risks and threats.

Content of audit report.

49. (1) The auditor report shall contain the following—

(a) any audit finding identified during the course of the audit;
(b) systemic finding, where the finding is spread throughout the critical information infrastructure, which could likely be a weakness in the design of the control;
(c) a recurring finding, including a finding brought up from past audits that have reoccurred in the current audit even after implementing the corrective action; and
(d) good practices, in areas of governance and controls, noted during the audit.

(2) The auditor shall give his opinion and recommendations on the following areas—

(a) appropriateness of the management comments in response to the audit finding;
(b) adequacy and effectiveness of the controls put in place by the owner of the critical information infrastructure to address

cybersecurity risks to the critical information infrastructure; and

(c) opportunities for improvement to secure the critical information infrastructure.

(3) The audit of critical information infrastructure undertaken under these Regulations may take any format provided that the elements specified under these Regulations are incorporated.

(4) Without prejudice to paragraph (3), the Audit report may be in the manner provided in Form CMCA 6 set out in the Third Schedule.

Procedure for submission of audit report.

50. (1) The Auditor shall within fourteen days upon completion of the audit exercise, furnish the Director with an audit report.

(2) The Director shall table the audit report before the Committee within seven days upon receipt thereof.

(3) Upon consideration of the audit report under paragraph (3), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the Committee.

(4) The recommendations by the Committee shall form the subject of evaluation by the auditor in the subsequent audit exercise.

(5) The Committee shall submit its reports to the National Security Council.

Division IV—National Public Key Infrastructure

National Public Key Infrastructure Components.

51. (1) In this Division—

"certification authority" means a licensed third party specialised in issuing and managing digital certificates;

"National Public Key infrastructure" means a system of policies, procedures, technology and services required to create, issue, manage, distribute and revoke digital certificates used to verify the online identity of individuals, organizations or devices by use of an identifiable public key cryptography to obtain secure communication;

"public key" means a technical infrastructure comprising of a Root Certification Authority and a Certification Authority or an Electronic Certification Service Provider;

"root certification authority" means the certification authority in a National Public key infrastructure responsible for issuing, managing and revoking digital certificate for certification authorities in the country.

(2) The National Public Key Infrastructure Components comprises—

(a) the National Bridge Certification Authority;
(b) the Sector Bridge Certification Authority;
(c) the Root Certification Authorities;
(d) the Certification Authority;
(e) the Registration Authorities; and
(f) the Subscribers.

(3) The National Public Key Infrastructure shall—

(a) be managed by use of a public and private Key; and

(b) be interoperable amongst other systems that support the secure development and use of systems.

(4) Despite paragraphs (1) and (2), the owners of critical information infrastructure shall use public key infrastructure controls, to safeguard the confidentiality, integrity and availability of the critical information infrastructure.

Responsibilities of the Committee on the National Public Key Infrastructure.

52. The Committee shall for purposes of managing the National Public Key Infrastructure—

(a) formulate the national public key infrastructure policies and standards;
(b) coordinate and supervise the national public key infrastructure framework;
(c) assign and oversee the certification authorities;
(d) designate and assign the functions of the national public key infrastructure to a public institution;
(e) receive biannual reports from certification authorities; and
(f) create awareness and build capacity on matters relating to the public key.

National Bridge Certification Authority.

53. The National Bridge Certification Authority shall -

(a) implement the National Public Key Infrastructure policies, rules and regulations;
(b) promote the use of Public Key Infrastructure technology to secure e-Government, e-Commerce, e-Banking and other services;
(c) establish trust paths amongst various Sector Public Key Infrastructures including the Foreign Certification Authority;
(d) issue keys and certificates to the Sector Public Key Infrastructures; and
(e) supervise compliance with the provisions of these Regulations.

Sector Bridge Certification Authority.

54. The Sector Bridge Certification Authority shall—

(a) be linked to the National Bridge Certificate Authority system;

(b) be organised in the accordance with the sectors specified in the Second Schedule;

(c) comprise Root Certification Authorities within the Sector;

(d) have member Sectors connected to the Sector Regulator or responsible line Ministry which shall be the Principal Root Certification Authority for the purposes of these Regulations;

(e) accredit certification authorities within the sector through issuance, revocation, suspension, or renewal of sector certificates;

(f) manage and maintain a register of certification authorities within the Sector;

(g) establish trust paths amongst various Sector Public Key Infrastructures including the Foreign Certification Authority;

(h) issue keys and certificates to the Sector Public Key Infrastructures; and

(i) perform such things as may be necessary for the implementation of these Regulations.

Root Certification Authority.

55. (1) A sector shall establish and operate a Root Certification Authority.

(2) The Root Certification Authority shall—

(a) regulate the sector public key infrastructure through accreditation and audit sector certification authority;

(b) generate, manage and distributes certification authorities and time stamping service providers;
(c) operate and manage the Root Certification Authority system and its functions;
(d) issue, renew and revoke accreditation to sector Certification Authority;
(e) develop technical requirements for Sector
(f) register cryptography service providers;
(g) monitor the conduct, systems and Operations of certification authorities, time stamping service providers and cryptography service providers to ensure compliance with these Regulations;
(h) appoint an independent auditing firm to conduct periodic audits of a certification authority to ensure compliance with the provisions of these Regulations;
(i) verify the accuracy of results of the information systems audit submitted to the Root Certification Authority;
(j) conduct inspections and audits;
(k) maintain a certificate revocation records and any other repositories;
(l) conduct research and development with regard to certification and cryptography services;
(m) issue sectoral guidelines in line with the national public key infrastructure;
(n) report, bi annually, the Committee; and
(o) regulate the provision of secure signature creation devices.

Certification Authority.

56. (1) A certification authority shall utilize a trustworthy system in performing its services and be either public body or private entities.

(2) A public certification authority shall generate, manage, issue and distribute public key infrastructure to public bodies.

(3) A private certification authority shall generate, manage, issue and distribute public key infrastructure to private bodies.

Registration Authority.

57. (1) The Certification Authority may appoint any person as a Registration Authority.

(2) The Registration Authority shall—

(a) verify the identity of individuals and organizations before issuing digital certificates;
(b) act as a trusted third party to ensure the authenticity and validity of the identity information provided;
(c) verify the identity of individuals before issuing digital signatures;
(d) identify subscribers;
(e) register or verify the applicant information;
(f) transmit the certificate request to Sector Certification Authority;
(g) validate certificates by the Sector Certification Authority;
(h) request for revocation, suspension and restoration of certificates;
(i) ensure that all aspects of registration services and operations are performed; and
(j) perform any other role specified by the other written laws.

Subscribers.

58. A subscriber shall, where the subscriber generates a key pair whose public key is to be listed in a certificate and accepted by the subscriber, generate that key pair using a trustworthy system.

PART V— CYBERSECURITY CAPABILITY AND CAPACITY

Cybersecurity capabilities.

59. (1) Pursuant to section 6 (1) (j) of the Act, the Committee shall formulate a National Cyber Protection Framework.

(2) The National Cyber Protection Framework shall provide a cyber-defense strategy for the Republic of Kenya.

(3) Without prejudice to the generality of paragraphs (1) and (2), the National Cyber Protection Framework shall—

(a) provide for a Training Guide on cybersecurity in Kenya;

(b) provide for information sharing arrangements amongst organization in the private and public sector including international organizations;

(c) formulate administrative guidance notes for addressing cyber-security and any matters of common interest in the sector, in consultation with the respective Regulators of a Sector;

(d) establish a Centre of Excellence which shall –

(i) formulate research codes on cybersecurity, in consultation with the Committee;

(ii) certify institutions and professionals suitable to train or consult on cybersecurity in Kenya; and

(iii) perform any other function that the Committee may consider necessary;

(e) research on emerging technologies and security solutions; and

(f) formulate cybersecurity technical certification standards for organizations.

Training Guide.

60. (1) The Committee, shall formulate a National Training Guide to provide tools and information required by training institutions on cybersecurity in the Country.

(2) The Training Guide shall—

(a) create public awareness of cybersecurity, cyber safety, and cyber ethics including continuous training of the contents of the Act and these Regulations;
(b) disseminate the cybersecurity technical standards and best practices formulated by the Committee;
(c) provide practical approach and best practices in cybersecurity usable by individuals, small to medium-sized businesses, educational institutions, the National Government and County governments and the private sector;
(d) support the development of a strategic approach on training in cybersecurity for all institutions of learning which shall be incorporated in the education policy, standards, curricula and examinations including –
    (i) facilitating national programs to advance cybersecurity education, training, and workforce development;
    (ii) supporting formal cybersecurity education and digital forensic programs and local certification programs at all educational levels to prepare and improve a skilled cybersecurity workforce for the private sector, the National Government and County Governments;
    (iii) recommend to the relevant regulatory bodies on the review and accreditation of academic and professional programs on cybersecurity in the country;

(e) identify and address cybersecurity workforce skill gaps in the public and private sectors;
(f) collaborate with the relevant Ministries, State or County Department or agencies at both levels of Government, in addressing sector specific needs of the cybersecurity workforce of critical information infrastructure, including cyber physical systems and control systems;
(g) develop metrics to measure the impact programs and initiatives in the Training Guide on the cybersecurity workforce; and
(h) promote initiatives to evaluate and forecast future cybersecurity workforce needs of the Country.

Framework for Information sharing arrangements.

61. The Committee shall for purposes of establishing effective practices to protect against cyber threats develop a framework for information sharing for —

(a) establishing trusted networks of information sharing partners including administrative guidelines for identifying trusted organizations;
(b) establishing relationships regarding the sharing of Cybersecurity information;
(c) providing early warning alerts, announcements and dissemination of information concerning risks and incidents;
(d) information sharing on situational awareness of computer systems vulnerabilities, threats, and incidents across the country and globally;
(e) explore credible information sharing platforms including encrypted messaging applications, threat intelligence platforms, secure web portals, recommendations on suitable tools based on an organizations size, resources and requirements; and
(f) convening meeting including colloquiums, webinars, seminars, workshops or conferences to share cybersecurity information.

Self-regulation.

62. The Committee shall promote self-regulation of the various sectors through—

(a) supporting the development of sector-based administrative guidelines to cater for cybersecurity of common interest within the sector;

(b) collaborating with the Regulators to promote Cybersecurity in each sector including ensuring adherence to the National Cybersecurity Strategy.

National Cybersecurity Certification Standards.

63. The Committee shall establish National Cybersecurity Certification Standards, in consultation with the relevant agencies for purposes of —

(a) attesting that the cybersecurity products, cybersecurity services and cybersecurity processes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle; or

(b) certifying relevant organizations that comply with the provisions of the Act and these Regulations.

Security automation and checklists for Government Systems.

64. (1) The Committee shall, develop security automation standards including —

(a) reference materials or protocols;

(b) checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool used by the National Government and county Governments, enabling standardized and interoperable technologies and architectures; and

(c) frameworks for continuous monitoring of information security within the country.

(2) The Standards referred to under paragraph (1) shall be based on—

(a) the security risks associated with the use of the system;
(b) the number of entities that use a particular system or security tool;
(c) the usefulness of the standards, reference materials, or checklists to the users or potential users of the system;
(d) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; and
(e) such other factors as the Committee determines to be appropriate.

(3) The Committee shall disseminate and make available the standards, reference materials, checklists, or other instruments developed under this regulation.

Collaboration by Committee.

65. The Committee shall collaborate with the relevant entities including—

(a) public bodies at the national and county governments;
(b) private sector entities,
(c) the Cybersecurity Operations Centers (CSOCs);
(d) owners of critical information infrastructure;
(e) international organizations; or
(f) and any other relevant industry organizations.

Collaboration with training institutions.

66. A cybersecurity or cybercrime training institution shall collaborate with the Committee in the development of cybercrime and cybersecurity modules of training and the mechanisms to assess the effectiveness of the cybercrime training.

Database of certified cybersecurity institutions and professionals.

67. The Committee shall maintain an up-to-date database of certified institutions and professionals suitable to conduct research or consult on cybersecurity in Kenya.

PART VI—CYBERTHREATS REPORTING MECHANISMS

Objectives of reporting of cyber threats.

68. The basis for reporting cyber threat as contemplated under section 40 of the Act shall be to –

(a) provide actionable information or complaints which can be the basis for investigations and prosecutions;

(b) identify cybercrime threats on citizens and organizations, understanding and measuring trends;

(c) establish a channel of communication between citizens including victims, witnesses of cybercrime and the law enforcement agencies;

(d) coordinate between law enforcement agencies and public authorities; and

(e) foster a culture of public and private sector cooperation and information sharing including international cooperation.

Reporting of cyber threats.

69. (1) In addition to the requirements provided under section 40 of the Act, a report on cyber threat, attack, intrusion, risk or other disruption or potential disruption shall be provided in Form CMCA 7 set out in the Third Schedule and shall specify—

(a) in case of an individual—

(i) full names;
(ii) email addresses;
(iii) phone number;
(iv) county;
(v) type of threat, attack, intrusion, risk or other disruption;
(vi) brief description of the threat, attack, intrusion, risk or other disruption;
(vii) date and time of the threat, attack, intrusion, risk or other disruption;
(viii) screenshots of suspicious activity, malicious URLs, malicious social media accounts; or
(ix) any other evidence.

(b) in case of an owner of a critical information infrastructure, official organization email addresses—

(i) official websites
(ii) phone number;
(iii) county;
(iv) type of threat, attack, intrusion, risk or other disruption;
(v) brief description of the threat, attack, intrusion, risk or other disruption;
(vi) date and time of the threat, attack, intrusion, risk or other disruption;
(vii) screenshots of suspicious activity, malicious Uniform Resource Locators

(URLs), malicious social media accounts; and

(viii) any other evidence.

(2) The incidence report may be made either by electronic means or physical means to the Committee.

Anonymous reporting of cyber threats.

70. (1) The Committee or any law enforcement agencies, or an organization, shall provide mechanism for anonymous reporting channels to allow any person to disclose useful information related to cyber incidents or crimes anonymously.

(2) For the avoidance doubt the anonymous reporting channels may include—

(a) social media platforms;
(b) telephone call;
(c) other electronic reporting channels; or
(d) any other mode convenient to the person reporting considering the circumstances of the cyber threat.

(3) Anonymous reporting under this regulation may include information on—

(a) the interruption of a life sustaining service including the supply of water, health services and energy;
(b) an adverse effect on the economy of the Republic;
(c) an event that would result in massive casualties or fatalities;
(d) failure or substantial disruption of the money market of the Republic; and
(e) adverse and severe effect of the security of the Republic including intelligence and military services;

(f) dangers of public health, safety and the environment; or
(g) any other information which may disrupt the confidentiality, integrity and availability of a computer system or a critical information infrastructure.

(4) A person shall not be penalized in relation to any employment, profession, voluntary work, contract, membership of an organization, the holding of an office or in any other way, as a result of reporting a cyber-threat which the person obtained in confidence in the course of that activity, if the reporting is in public interest.

(5) For purposes of paragraph (4), a report which is made to the Committee, a law enforcement agency or to an appropriate entity shall be deemed to be made in the public interest.

(6) A person shall report a cyber-threat under this regulation where such person has reasonable belief in the veracity of the information.

(7) Any person who provides false information maliciously intended to injure another person commits the offence specified under section 22 of the Act.

(8) For the purpose of paragraph (4), a person is penalized if the person is dismissed, discriminated against, made the subject of reprisal or other form of adverse treatment or is denied any appointment, promotion or advantage that otherwise would have been provided or any other personnel action provided under the law relating to whistle blower, and the imposition of any such penalty in contravention of this section shall be actionable as a tort.

PART VII—MISCELLANEOUS PROVISIONS

Adoption of best practice standards.

71. (1) Subject to paragraph (2), the Director shall periodically identify and evaluate global cybersecurity best practices and standards and recommend the adoption by the Committee.

(2) The Committee may formulate codes of practice or standard operating procedures based on the recommendations under paragraph (1) which shall be applicable to the various sectors including owners of critical information infrastructure.

(3) Despite paragraph (2), organizations or owners of critical information infrastructure may on their own initiative identify, evaluate and adopt global best practices and standards on cybersecurity.

Partnerships and linkages.

72. Pursuant to section 12 of the Act, the Committee may enter into public-private partnerships and intergovernmental, agreements, partnerships, linkages or collaborations as provide for under the relevant laws to—

(a) improve local, regional or global response to cyberattacks or prevent cybercrime;
(b) build cybersecurity capacity;
(c) address emerging issues arising from cybercrimes; or
(d) to give effect to the objects of these Regulations.

Dispute resolution mechanism.

73. (1) A person aggrieved by a decision of any person under these Regulations may apply to the Cabinet Secretary to review the decision within seven days from the date the decision was made.

(2) The Cabinet Secretary shall within thirty days make a determination on the application for review submitted under paragraph (1).

(3) Despite paragraph (1), the Committee may on own motion review any decision made under these Regulations any of the following grounds—

(a) a mistake or error apparent on the face of the record;

(b) discovery of new and important matter of evidence; or

(c) any other sufficient reason.

(4) A person dissatisfied with the decision of the Committee or Cabinet Secretary may appeal to the High Court within thirty days from the date of the decision.

Data Protection. *No.24 of 2019.*

74. The Data Protection Act, 2019 shall apply to processing of personal data pursuant to the Act and these Regulations.

FIRST SCHEDULE (r.7)

CONDUCT OF BUSINESS AND AFFAIRS OF THE COMMITTEE

1. Notice of meetings

(1) Except in the case of a special meeting, at least seven days' written notice of a meeting of a body shall be issued to each member of the Committee.

(2) In the case of a special meeting, the chairperson shall convene an *ad hoc* meeting upon receipt of the requisition for the special meeting.

2. Quorum

The quorum for the conduct of the business of a meeting of Committee shall be six members of the total membership.

3. Conduct of meetings

(1) The chairperson of the Committee shall, in consultation with the Director—

(a) determine the agenda of the meetings of the Committee including the date, time and venue of the meeting; and
(b) convene and chair the meetings.

(2) In the absence of the chairperson at a meeting of a Committee, the members present shall elect a member to chair the meeting of meetings.

4. Voting

(1) The decisions of the Committee shall be by a majority of the members present during a meeting.

(2) In the event of an equality of votes, the Chairperson, or other person presiding, shall have a casting vote.

5. Attendance by non-members

The Committee may invite a person who is not a member of the Committee to attend and participate at a sitting of the Committee but such person shall not be entitled to vote.

6. Committees

A meeting of the Committee may establish standing or ad-hoc committees charged with specific responsibilities.

7. Conflict of Interest

(1) Any member of the Committee who has an interest in any matter that may be in conflict with the Operations of the Committee shall disclose the conflict to the other members of the Committee and refrain from taking part, or taking further part, in the consideration of the matter.

(2) A disclosure of interest shall be recorded in the minutes of the meeting at which it is made.

8. Records of meetings

The Secretariat shall maintain clear and accurate minutes of the meetings of the Committee and all other records that relate to the work of the Committee.

9. Confidentiality

The members of the Committee shall maintain the confidentiality and integrity of all communications and deliberations of the Committee.

10. Other procedure

Except as provided in this Part, the Committee may regulate its own procedure.

SECOND SCHEDULE **(**r.11, 20 & 52)

CRITICAL INFORMATION INFRACSTUCTURE SECTORS

A system or critical infrastructure that is essential to the provision of the following critical services is designated as critical information infrastructure in accordance with these Regulations and the Act—

	Critical Sector	**Critical Subsector**	**Critical Services**
1.	**Energy.**	Electricity	(a) Generation (all forms) (b) Transmission /Distribution (c) Electricity Market
		Petroleum	(a) Extraction (b) Refinement (c) Transport (d) Storage
		Natural Gas	(a) Extraction (b) Transport / Distribution (c) Storage
2.	**Information, Communication Technologies (ICT)**	Information Technologies	(a) Web services (b) Data centre/ cloud services (c) Software as a Service
		Communications	(a) Voice/ Data communication (b) Internet connectivity

3.	**Water.**	Drinking water	(c) Water storage (d) Water Distribution (e) Water Quality Assurance
		Waste Water	Waste water collection and treatment.
4.	**Food**		(a) Agriculture /Food production (b) Food supply (c) Food distribution (d) Food quality/safety
5.	**Health**		(a) Emergency healthcare (b) Hospital care (inpatient & outpatient) (c) Supply of pharmaceuticals, vaccines, blood, medical supplies (d) Infection/epidemic control
6.	**Financial Services.**		(a) Banking (b) Payment transactions (c) Stock Exchange
7.	**Transport.**	Aviation	(a) Air navigation services (b) Airports Operations
		Road transport	(a) Bus services/Matatu

			(b) Maintenance of road network
		Train transport.	(a) Management of public railway (b) Railway transport services
		Maritime transport	(a) Monitoring and management of shipping traffic. (b) Docking
		Postal/shipping	
8.	**Industry**	Critical industries	Employment
		Chemical/Nuclear Industry	(a) Storage and disposal of hazardous materials (b) Safety of high-risk industrial units
9.	**Space**		Protection of space-based systems
10.	**Environment**		(a) Air pollution monitoring and early warning (b) Meteorological monitoring and early warning (c) Lake/ River (Ground) Water monitoring and early warning

			(d) Marine pollution monitoring and control.
11.	**Public Order and Safety**		(a) Maintenance of public order and safety. (b) Judicial systems
12.	**Civil Protection**		Emergency and rescue services
13.	**Civil Administration**		(a) National Government functions (b) County governments functions
14.	**Education**		(a) Early learning (b) Basic Education (c) Vocational and technical training (d) University education
15.	**Election**		(a) Registration of voters (b) Voting
16.	**Defense**		National defense

THIRD SCHEDULE

FORMS

FORM CMCA 1 (r.24(2)(a))

APPLICATION FOR DESIGNATION OF CRITICAL INFORMATION INFRASTRUCTURE

Organization Details

Name of the Organization…….

Sector it belongs;

(a) Telecommunications Sector
(b) Electoral, Judicial, Education, Health, Food, Water, and Land Sector
(c) Energy, Transport, and Industry Sector
(d) Banking and Finance Sector
(e) Defense, Security, and Public safety sector

Reasons why you are considering yourself Critical;

Can disruption of the system/Service result in—

(a) the interruption of a life-sustaining service
(b) including the supply of water, health services and
(c) energy;
(d) an adverse effect on the economy of the Republic;
(e) an event that would result in massive casualties or
(f) fatalities;
(g) failure or substantial disruption of the money
(h) the market of the Republic; and
(i) adverse and severe effect of the Security of the
(j) Republic, including intelligence and military services.

Provide a comprehensive list of the systems, networks, databases, applications, and other critical assets.

(a) …….
(b) ……
(c) ……..

(d) …….
(e) …….

Services

List all the Critical Services you are offering.

(a) …….
(b) ……
(c) ……
(d) ……..
(e) ……..

Briefly Describe the services bringing out the criticality aspect.

List all the Systems/Information Infrastructure Running

(a) ……
(b) ……
(c) …….
(d) ……
(e) …….

Describe why the Systems/Information Infrastructure are critical in your day-to-day Operations.

Who manages the Systems/Information Infrastructure?

Name:

Phone Number:

……

Email address:

……

Systems/Information Infrastructure

Where does your data reside currently?

(a) Cloud

(b) In-house

If Cloud, which ones?

(a) . ……
(b) ……
(c) ……
(d) ……
(e) ……

If in-house, what measures are taken to safeguard/ensure data protection?

(a) ……
(b) ……
(c) ……
(d) ……
(e) ……

How is data backup and data protection handled?

Do you run Systems/Information Infrastructure audits?

(a) If yes, How often?
(b) Annually
(c) Semi-Annually
(d) How is it done?

Is there continuous monitoring and threat detection in place?

People

What training and awareness programs are currently in place?

(a) ……
(b) ……
(c) ……
(d) ……
(e) ……

Describe the incident management and response procedures in place to address cybersecurity incidents or breaches.

Highlight the organization's ability to coordinate with relevant authorities and stakeholders in the event of a cybersecurity incident.

Provide any compliance certifications or accreditations relevant to the CII designation.

(a) ……
(b) ……
(c) ……
(d) ……
(e) ……

Include information on how the organization adheres to relevant cybersecurity regulations and guidelines.

Include any additional documents, reports, or evidence substantiating the organization's CII designation eligibility.

FORM CMCA 2 **(r.27(2) & 28 (1))**

APPLICATION FOR CHANGES IN THE DESIGN OR OWNERSHIP OF A CRITICAL INFORMATION INFRASTRUCTURE

A. General Information	
Application for changes in:	☐ Design of a Critical Information Infrastructure ☐ Ownership of a Critical Information Infrastructure
B. Applicant Information	
Name	
Telephone	
Email Address	
C. Critical Information Infrastructure (CII) Details	
Name of organization	
Address of organization	
Name of CII	
Location of CII	
D. PROPOSED CHANGES TO DESIGN OF THE CII	
Detailed description of proposed changes in design of CII	
Justification for proposed changes in design of CII	

Timeline for implementing the changes	
E. **Proposed changes in ownership of the CII**	
Proposed new owner	
Reason for change in ownership	☐ Acquisition and mergers ☐ Strategic partnership ☐ Ownership transfer/ succession ☐ Regulatory requirements/compliance ☐ Others (Specify)

F. **DECLARATION**

I, ----------, hereby declare and affirm that all the information provided in this application for changes in the design or ownership of the Critical Information Infrastructure (CII) is true, accurate, and complete to the best of my knowledge.

I am duly authorized to submit this application on behalf of the organization, ----------, and I assume full responsibility for the accuracy and authenticity of the information presented herein. I declare that no information has been withheld or misrepresented that could adversely affect the integrity or evaluation of this application.

Applicant Signature ---------- Date ----------

FOR OFFICIAL USE

Application received by name _____ Signature _____ Date _____

Remarks

_____

G. Authorization

I hereby authorized the proposed changes in CII design/ownership.

Signature

Director

National Computer and Cybercrimes Coordination Committee

FORM CMCA 3 (r.29(2))

APPLICATION FOR CHANGES LOCATION OF A CRITICAL INFORMATION INFRASTRUCTURE

ORGANIZATION BASIC INFORMATION

Name of Organization:

_____

Sector:

_____

Address: _____

S/No.	**MOVE FROM CURRENT LOCATION** Building/ Floor/ Room	**MOVE TO NEW LOCATION** Building/ Floor/ Room
1.		
2.		
3.		
4.		
5.		
OLD CUSTODIAN		**NEW CUSTODIAN**
NAME:		NAME:
CONTACT:		CONTACT:

REASON FOR CHANGE IN LOCATION

_____

_____

_____

_____

_____

_____

FEATURES

S/No.	CURRENT LOCATION	NEW LOCATION
1.		
2.		
3.		
4.		
5.		

Dept. Release Signature: _____ Dept. Acceptance Signature: _____

Date: _____ Date: _____

Approved by: _____ Signature: _____

Date: _____

EQUIPMENT RELOCATION FORM
EQUIPMENT RELOCATION ITEMIZED LIST

S/NO	EQUIPMENT	MODEL	MANUFACTURER	SERIAL NO.	TAG NO.	FROM	TO
1.							
2.							
3.							
4.							
5.							
6.							

7.							
8.							
9.							

FORM CMCA 4 (r.44(4))

APPOINTMENT CERTIFICATE FOR AN AUDITOR

A. PARTICULARS OF THE APPOINTING ORGANIZATION	
Name of the organization	NC4
Postal Address	
Phone Number	
Email Address	
B. PARTICULARS OF THE AUDITOR	
Full Names	
National Identification Card Number/Passport Number	
Postal Address	
Phone Number	
Email Address	
Roles/Responsibilities	
C. PARTICILARS OF THE ORGANIZATION TO BE AUDITED	
Name of the organization	
Postal Address	
Phone Number	
Email Address	
D. DURATION	
Start Date	
End Date	

E. DECLARATION

I, [Name of the Appointee], hereby accept the appointment as a Critical Information Infrastructure Auditor and confirm my commitment to fulfill the responsibilities entrusted to me to the best of my abilities.

F. APPROVAL

Date of Approval:

Director

National Computer and Cybercrimes Co-ordination Committee

FORM CMCA 5 (r.46(2))

NOTICE TO CONDUCT AUDIT BY THE DIRECTOR

A. PARTICULARS OF THE APPOINTING ORGANIZATION	
Name of the organization	NC4
Postal Address	
Phone Number	
Email Address	
Website	
B. PARTICILARS OF THE ORGANIZATION TO BE AUDITED	
Name of the organization	
Postal Address	
Phone Number	
Email Address	
C. PURPOSE OF AUDIT	
D. AUDIT SCOPE	
E. DURATION	
Start Date	
End Date	

F. SUBJECT

As part of our ongoing commitment to ensuring transparency, accountability, and adherence to best practices, we are hereby notifying you of the decision to conduct an audit of your Critical Information Infrastructures (CIIs) at [Organization's Name].

G. APPROVAL

Date of Approval:

Director

National Computer and Cybercrimes Co-ordination Committee

FORM CMCA 6 **(r.49(4))**

TEMPLATE OF AUDIT REPORT

Section 1: Contact/Demographic Information				
1.1 Details of the auditor				
Name of the Auditor				
Organizational Affiliation				
Contact Details	Telephone			
	Email			
Date audited(dd/mm/yyyy)				
1.2 Details of the organization audited				
Name of organization				
Address of organization				
Name of CISO				
Contact Details of CISO	Phone		Email	
Contact Detail of the officer in charge of the audit at the organization(Point of contact)	Phone		Email	
Type of organization	☐ GoK ☐ Critical Information Infrastructure ☐ Private Sector			
Section-2: Introduction				
2.1 Purpose of the Audit				

2.2 Scope of the Audit	
2.3 Methodology	
Section-3: Audit Findings	
3.1 Network Security	3.1.1 Firewall Configuration and Rules
	3.1. 2 Intrusion Detection and Prevention Systems (IDPS)
	3.1.3 Network Access Control
	3.1.4 Wireless Network Security
	3.1.5 VLAN Segmentation
3.2 System(s) Security	3.2.1 Operating System Patching and Updates

	3.2.2 Antivirus and Endpoint Security
	3.2.3 Secure Configuration of Servers and Endpoints
	3.2.4 Access Control to Critical Systems
3.3 Data Security	3.3.1 Data Classification and Handling
	3.3.2 Data Encryption (at rest and in transit)
	3.3.3 Data Backup and Disaster Recovery
3.4 Application Security	3.4.1 Secure Coding Practices
	3.4.2 Web Application Security
	3.4.3 Application Authentication and Authorization
3.5 Physical Security	3.5.1 Access Control to Data Centers and Server Rooms
	3.5.2 Surveillance and Monitoring
Section 4: Risk Assessment	
4.1 Identified Risks	
4.2 Risk Analysis/Posture	

4.3 Risk Mitigation Recommendations	
Section 5: Compliance Assessment	
5.1 Regulatory Compliance	
5.2 Industry Standards (e.g., ISO 27001, NIST, etc.)	
Section 6:Conclusion	
6.1 Summary of Findings	
6.2 Strengths and Weaknesses	
6.3 Recommendations	
Section 7: Appendices	
7.1 Detailed Audit Methodology	
7.2 Glossary of Terms	
7.3 References	

FORM CMCA 7 **(r.69(1))**

REPORTING TEMPLATE FOR A CYBER THREAT OR CYBER ATTACK

Type of Report	☐ Initial ☐ Follow up ☐ Final	**Classification of Document**	☐ Restricted ☐ Confidential ☐ Secret ☐ Top Secret

Section-A: General Information					
I am: ☐ The impacted user ☐ Reporting on behalf of the impacted user					
Reason for reporting; ☐ To inform NC4 on the incident ☐ To request incident response assistance					
Name					
Telephone					
Email Address					
	Impacted organization Details				
Name of organization					
Address of organization					
Name of CISO					
Contact Details of CISO	Phone		Email		
Contact Detail of Officer in charge of the incident(Point of contact)	Phone		Email		
Type of organization	☐ GoK ☐ Critical Information Infrastructure ☐ Private Sector				
Location of the incident					
	Incident Description				

When, approximately, did the incident start?	Date		Time	
When was the incident detected	Date		Time	

Type of incident(✓Check mark)

☐	Website Defacement	☐	Un-patched Vulnerable Software Exploitation
☐	Patched Software Exploitation	☐	Unauthorized System Access
☐	Exploitation of Weak Configuration	☐	Data Theft
☐	Account Compromise	☐	Malware Infection

☐	Service Disruption	☐	Wireless Access point Exploitation
☐	Social Engineering and Phishing Attacks	☐	Exploitation of Weak Network Architecture
☐	Unintended Information Exposure	☐	Network Penetration
☐	Spoofing or DNS Poisoning	☐	Any other (Please describe below)

4. Brief description of the incident

5. Interface affected	☐	Public Network	☐	Internal Network	☐	Other

6. Incident Handling Steps taken

a) Immediate	

b) Long term	
c) Recovery steps taken	

7. Has any third party been informed? (If Yes, please list all third parties that have been informed about this incident so far)

Third party contacted	Role of third party

Section-B: Impact Details

Incident impact on the organization's business				
Technical impact on the organization	☐ Information/ Data theft ☐ Service Disruption (Downtime) ☐ System(software/hardware) Sabotage ☐ Other (Specify)			
Number of systems impacted				
Number of people impacted				
Assessment of risk of harm to individuals	☐ No harm to individuals ☐ Minimal harm to individuals ☐ Fatal harm to individuals			
Time of Incident resolution	From dd/mm/yy, hh:mm		To dd/mm/yy, hh:mm	

Made on the ……., 2023.

KITHURE KINDIKI,
Cabinet Secretary for Interior and National Administration.