LEGAL NOTICE NO. 44

THE COMPUTER MISUSE AND CYBERCRIME (CRITICAL INFORMATION INFRASTRUCTURE AND CYBERCRIME MANAGEMENT) REGULATIONS, 2024

ARRANGEMENT OF PARAGRAPHS

Regulation

THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

(No. 5 of 2018)

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

PART I— PRELIMINARY PROVISIONS

Citation.

1. These Regulations may be cited as the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024.

Interpretation.

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

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

"accreditation certificate" means an accreditation certificate issued by the Information and Communication Technology Authority established under the Information and Communications Technology Order, 2013;

No. 5 of 2018.

"attribution" includes the process of tracking and identifying the perpetrators of a cyber-attack;

L.N. 182 of 2013.

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

"certificate practice statement" means the rules and operating practices guiding the Certification Authority in providing digital certificate services which may include a description of service offered, detailed procedures for certificate lifecycle management, operational information, legal obligations or financial liabilities;

"certificate policy" means a set of rules that indicate the applicability of the certificate practice statement to a particular community or class of applications with common security requirements;

"Chief Information Security Officer" means the person designated or appointed as a Chief Information Security Officer pursuant to regulation 32;

"critical information infrastructure" means a system designated pursuant to section 9 of the Act and includes critical information infrastructure system or data and national critical information infrastructure;

"cybersecurity" means tools, policies, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies utilized to protect the cyber environment;

"cryptography" includes the use of systems to secure information or data;

"cybersecurity incident" means an occurrence that—

(a) jeopardizes without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

"Cybersecurity Operations Centre" means the capability that encompasses cutting-edge technology, tools and a team of cybersecurity experts organized to protect, monitor, detect, analyse, respond and report on cybersecurity incidents and threats;

"cybersecurity service provider" means a third-party individual or organization that provides security services to secure critical information infrastructure against potential cyber security threats;

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

"digital trust" means user confidence in the security, fairness and reliability of digital environments established through actions, controls and behaviour of the personnel in an organization;

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

"emerging technologies" means the application of new technologies and ongoing developments in the use of existing technologies that have the potential to impact cybersecurity;

"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.

"imminent threat" includes an occurrence that actually jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system;

"information system" means an integrated set of components of technology, data and procedures for processing information which includes collecting, storing, and disseminating information;

"international internet gateway" means any facility that provides an interface to send and receive electronic communication traffic between one country's domestic network facilities and those in another country;

"internet gateway" means devices or systems that serve as entry and exit points between different networks, and allows data flow between networks to facilitate communication between networks that use different protocols or technologies, ensuring that information may be routed and transmitted;

"internet protocol address allocation" means the allocation of the unique identifying number assigned to every device connected to the internet;

"internet service provider" means a company that provides access to the internet through multiple means, including wireless and fiber-optic connections;

"national internet gateway" means the internet gateway owned and operated by the Government of Kenya;

"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;

"network equipment interface" means a device that serves as the demarcation point between the internet gateway and the customer's premises wiring;

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

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

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

"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 contained in a National Public Key Infrastructure as provided under regulation 51;

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

"subscriber" means a person that has applied for and issued with a digital certificate from a Certification Authority;

"system" means the digital or physical components that comprise a critical information infrastructure;

"third party" means an external entity having a written or implied contractual relationship with the first-party organization and may include service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors;

"tool engineering" includes developing and testing new designs in relation to cybersecurity and carrying out quality assurance tests;

"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;

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

(c) cause it to be an output from a 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 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 a framework for the 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 contained in the national 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 the 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) coordination in cyber security, defense, resilience, and other operations 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, by ensuring the confidentiality, integrity, and availability of critical information infrastructure;

(e) minimization of the likelihood and impact of successful cyber-attacks;

(f) respect for the rights of individuals including privacy, human dignity, equity and social justice;

(g) good governance and integrity; and

(h) mutual trust amongst stakeholders, including government agencies, private sector, and the public, in cybercrime management and the management and protection of critical information infrastructure.

Scope of Regulations.

5. These Regulations shall apply to cybersecurity matters in the public sector and private sector, particularly—

(a) the members of the public;

(b) the owners of critical information infrastructure;

(c) cybersecurity internet service providers offering services provided under the Act and these Regulations; and

(d) any other relevant sector or entity.

PART II—ADMINISTRATION AND MANAGEMENT OF THE COMMITTEE

Responsibilities of the Committee.

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

(a) issue prompt and timely advice to the Government on cybersecurity strategies relating to various technologies and sectors;

(b) undertake advocacy and create public awareness on cybersecurity matters;

(c) receive and approve reports from the Cybersecurity Operations Centres;

(d) in collaboration with relevant agencies, formulate Information Security Standards;

(e) approve the identification and designation of critical information infrastructure;

(f) formulate codes of cybersecurity practice and standards of performance for owners of critical information infrastructure and sectors;

(g) review the compliance reports submitted by the owners of the critical information infrastructure in accordance with section 13 (1) of the Act;

(h) evaluate audit reports submitted by the Secretariat on designated critical information infrastructure;

(i) approve the development and management of the National Public Key Infrastructure Frameworks;

(j) 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;

(k) consider reports on emerging technologies and their impacts on security for informed decision making; and

(l) co-ordinate cybersecurity research undertaken by the Secretariat and consider the research for informed decision making.

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

(a) report to the National Security Council on all cyber incidents reported by the Cybersecurity Operations Centres that threaten 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 codes of cybersecurity practice and standards operating procedures for the Cybersecurity Operations Centres.

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 performing 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 circulate 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) facilitate in collaboration with relevant agencies, implementation of the Government of Kenya Information Security Standards;

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

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

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

(i) keep and maintain a database on critical information infrastructure and on reported cyber threats and incidences including the action taken;

(j) where necessary, provide technical or non-technical support to Cybersecurity Operations Centres;

(k) prepare sector administrative guidelines for the effective implementation of the Act and these Regulations;

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

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

(n) in consultation with the Committee, organize forums that facilitate information sharing with stakeholders; and

(o) receive and analyse reports and prepare policy briefs for consideration by the Committee.

PART III—CYBERSECURITY OPERATIONS CENTRES

Cybersecurity Operations Centres.

9. (1) 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 specified under paragraph (2).

(2) The Cybersecurity Operations Centres contemplated under paragraph (1) shall include—

(a) National Cybersecurity Operations Centre;

(b) Sector Cybersecurity Operations Centres; and

(c) Critical Information Infrastructure Cybersecurity Operations Centres.

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

(a) real time event monitoring, analysis, log collection and aggregation;

(b) an alert system;

(c) cybersecurity specialists organized to prevent, detect, analyse and respond to threats;

(d) asset inventory;

(e) vulnerability management;

(f) network detection and response;

(g) end point detection and response;

(h) intrusion detection;

(i) malware analysis and testing;

(j) threat prevention, monitoring and detection;

(k) incidence response and management; and

(l) threat intelligence platform.

National Cybersecurity Operations Centre.

10. (1) A National Cybersecurity Operations Centre shall be the national focal point for monitoring, detecting, preventing, responding, investigating and attribution of cyber threats, computer and cybercrimes 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 Centres and Critical Information Infrastructure Cybersecurity Operations Centres;

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

(c) co-ordinate response to cybersecurity incidents within the Sector Cybersecurity Operations Centres and Critical Information Infrastructure Cybersecurity Operations Centres including—

(i) co-operating with computer incident response teams through sharing of threat intelligence to inform response to cyber incidents;

(ii) receiving real-time information on cyber threats and incidents from the Cybersecurity Operations Centres;

(iii) threat and information sharing;

(iv) incidence response coordination;

(v) joint exercises and training of the Cybersecurity Operations Centres; and

(vi) 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 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 cooperation 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; and

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

Sector Cybersecurity Operations Centres.

11. (1) For the avoidance of doubt —

(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,

shall be deemed the Sector Cybersecurity Operation Centre.

(2) A Sector Cybersecurity Operations Centre shall be responsible for monitoring, detecting, preventing, responding and investigating cyber threats, that are specific to their respective Sector.

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

(a) collaborate, through information and threat intelligence sharing, within 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 Centres 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 collaboration, consultation 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 and best practices on emerging issues in the Sector;

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

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

(f) co-ordinate sectoral threat, monitor and respond to incidences in the Critical Information Infrastructure Cybersecurity Operations Centres in their respective Sector including—

(i) collecting, analysing and responding to threats reported by the Critical Information Infrastructure Cybersecurity Operations Centres;

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

(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 Centre 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; and

(l) facilitate the implementation of standards operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centres.

(4) The costs of operating each Sector Cybersecurity Operations Centre, shall be borne by the Regulator of the respective sector.

Critical Information Infrastructure Cybersecurity Operations Centre.

12. (1) A Critical Information Infrastructure Cybersecurity Operations Centre shall be responsible for monitoring, detecting, preventing, responding and investigating of cyber threats, in a Critical Information Infrastructure.

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

(a) provide real-time information on cyber threats and incidents to the National Cybersecurity Operations Centre and Sector Cybersecurity Operations Centre;

(b) collaborate with the relevant agencies, on cyber threat surveillance and analysis;

(c) have the requisite capability to detect, monitor, prohibit, prevent, respond and investigate cyber threats, computer and cybercrimes in the concerned organization;

(d) be responsible for incidence detection, analysis and response in the organization;

(e) undertake capacity building programs, research and development activities on cyber threats and incidents in the organization;

(f) report to the respective Sector Cybersecurity Operations Centre on all cyber incidents reported in the organization;

(g) undertake research and development for tool engineering;

(h) co-operate with other Critical Information Infrastructure Cybersecurity Operations Centres in the concerned Sector;

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

(j) implement the codes or standard operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centres.

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

Outsourced capabilities.

13. (1) An owner of a critical information infrastructure who intends to outsource services from an external service provider shall, in writing, notify the Committee prior to outsourcing.

(2) The owner of a critical information infrastructure shall enter into a written agreement with the external service provider 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 cybersecurity capabilities.

(4) Where the service involves granting access of the database to the external service provider, the owner of a critical information infrastructure shall prior to entering into an agreement with the external service provider—

(a) assess the cybersecurity risks involved in the engagement; and

(b) ensure that the external service provider undertakes to mitigate the risks identified under paragraph (a) and consents to—

(i) limitation of the data that the external service provider may process and the permitted purposes of its use as specified in the agreement;

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

(iii) the nature of processing activities that the external service provider may perform;

(iv) the duration of the agreement;

(v) the processing of the data at the conclusion of the agreement including submission of the data to the owner of critical information infrastructure;

(vi) the destruction or disposal of any material at the end of the contract and the reporting requirement to the owner of a critical information infrastructure;

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

(viii) the use of data and the implementation of data security measures specified in the agreement.

(5) Where an owner of critical information infrastructure permits an external service provider to provide a service through another entity, it shall be the duty of the owner of critical information infrastructure to include in the agreement the obligations and all the matters detailed in these Regulations of other entity in the agreement.

(6) The external service provider shall, on a quarterly basis, notify to the owner of the critical information infrastructure, on the status of implementation of their obligations under the agreement and on any cybersecurity incident.

Monthly briefs and compliance reports.

14. (1) The Cybersecurity Operations Centres specified under regulation 9 (2) 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 information on cyber risks, threats and incidents experienced by the respective Cybersecurity Operations Centres.

Monitoring and inspection of the Cybersecurity Operations Centres.

15. Subject to section 13 (3) of the Act, the Director shall in collaboration with the relevant sector Regulator, and on an annual basis, monitor and inspect any Cybersecurity Operations Centres to ensure compliance with the Act and these Regulations.

Technical support to Cybersecurity Operations Centres.

16. Where there is an imminent threat in the nature of a cyber-attack that may result to a computer and cybercrime to any Cybersecurity Operations Centre, the Director may upon request, inquire or provide the requisite technical or non-technical support to the Cybersecurity Operations Centre.

Risk assessment and evaluation of Cybersecurity Operations Centres.

17. (1) An owner of a critical information infrastructure shall, on an annual basis, 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 owner of critical information infrastructure shall undertake a risk assessment within twelve months from the date of commencement of these Regulations.

(3) The cyber-risk assessment contemplated under paragraph (1) 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) analyse 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 a critical information infrastructure 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 owner of critical information infrastructure 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 (5) 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 address any identified deficiencies.

(7) The Committee may reject a risk register where—

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

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

PART IV—CRITICAL INFORMATION INFRASTRUCTURE

Designation of critical infrastructure.

18. (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; and

(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.

(2) The Director shall designate a critical information infrastructure in the manner specified in the Act and these Regulations.

(3) The criteria under section 9 (2) of the Act shall guide the classification of a critical information infrastructure.

(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.

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

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

Directives upon designation.

20. (1) The Director shall, within thirty days of issuing the notice under regulation 19, 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 annual risk assessment;

(b) develop incidence response plans;

(c) implement suitable security measures; and

(d) ensure personnel are adequately trained in security best practices.

Failure to implement directives.

21. (1) The Director shall upon expiry of the timelines where the owner has failed to implement the directives, issue a notice to show cause to the owner of critical information infrastructure.

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

No. 4 of 2015.

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

(a) requirement to provide a detailed report on non-compliance to the National Security Council;

(b) recommendation to the respective sector Regulator to impose specific actions under their respective law;

(c) constitution of a multi-agency committee to implement the directives;

(d) full implementation of the directives by the Director; or

(e) recommendations to conduct investigations by the law enforcement agencies.

(4) Where an owner of a critical information infrastructure is dissatisfied with the decisions of the Committee, the owner may appeal to the High Court.

Gazettement of critical information infrastructure.

22. (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 the critical infrastructure in accordance with the procedure outlined in these Regulations.

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

Application by owner of critical information infrastructure.

23. (1) An owner of a critical information infrastructure may, in writing, apply to the Director to declare 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) specify details on the resources available to the owner or person in control of the system to—

(i) safeguard the system against destruction, disruption, failure or degradation;

(ii) repair or replace the system, including the critical infrastructure's equipment, materials or service; or

(iii) recover the system from any destruction, disruption, failure or degradation; and

(e) 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.

24. (1) Upon receiving an application for declaration of a system as critical information infrastructure under section 9 of the Act, the Director shall—

(a) be guided by the criteria specified 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;

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

(iii) the extent to which the designation as critical

(2) 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.

(3) Where the Director declines the application for designating a system as a critical information infrastructure, the Director shall, in writing, notify the applicant of the decision with reasons within thirty days.

(4) Where an applicant is dissatisfied with the decision under paragraph (3), the applicant may apply the provision of regulation 73 on dispute resolution.

Register of critical information infrastructure.

25. (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, 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.

26. (1) In this regulation–

"significant change" means a new system, integration or modification whose new functionalities may compromise the confidentiality, integrity and availability of the critical service.

(2) An owner of a critical information infrastructure shall not make any significant changes to the design, configuration, security or operations of a critical information infrastructure, without prior notification to the Director.

(3) The notification contemplated under paragraph (2) shall be in Form CMCA 2 set out in the Third Schedule and shall specify the reason for the changes to the critical information infrastructure.

(4) The Director shall upon receiving the notification submitted under paragraph (3) consider the following—

(a) evaluate the implications of the proposed changes to the operations, personnel, and infrastructure of the critical information infrastructure;

(b) whether there may 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.

(5) The Director may, pursuant to a notification issued under paragraph (2), provide feedback to an owner of a critical information infrastructure, within seven days of receipt of the notification.

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

Change of ownership.

27. (1) Where there is an intention to change 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 23.

(3) 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 notify the Committee through Form CMCA 2 set out in the Third Schedule.

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

Localisation of critical information.

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

(2) Without prejudice to paragraph (1), an owner of a critical information infrastructure who intends to have critical information located outside Kenya, shall apply the Committee in Form CMCA 3 set out in the Third Schedule.

(3) The Committee shall consider the application submitted under paragraph (2), and verify that it meets the security standards provided under the Act and these Regulations, and shall communicate its decision within thirty days of receipt of the notification.

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

(a) the security measures and safeguards being applied to the critical information infrastructure on which the information is contained meet the standards set out in the Act and these Regulations;

(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; and

(f) submissions by any concerned operator.

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

Obligations of owners.

29. (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 to ensure—

(a) the physical security of the hardware and other details of the 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) the facilitation of prompt access to the critical information infrastructure by authorized persons in the event of a cybersecurity incident or during auditing for compliance under section 13 of the Act;

(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) conduct of risk assessment identifying risk based security factors necessary to protect public health and safety, or national socio-economic security, where applicable; or

(i) utilize innovative methods available in the market of securing the critical information infrastructure against cyber-attack.

(3) 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.

Capacity building by owners of

30. (1) The owner of a critical information infrastructure shall—

(a) formulate their respective administrative instruments or standard operating procedures which may include best practices and code of ethics for adherence by users or operators of the Critical Information Infrastructure; and

critical information infrastructure.

(b) formulate and implement a cybersecurity awareness programme to create cybersecurity awareness for all persons who use, operate and manage the critical information infrastructure including—

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

(ii) provide regular and timely communication covering general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations; and

(iii) guide individual behaviour and the security.

(2) The cybersecurity awareness programme referred to under paragraph (1) (b) shall include the following topics—

(a) cybersecurity;

(b) identification and reporting suspicious activity;

(c) incident management and response;

(d) insider threats;

(e) best practices from each Sector including physical security of the critical information infrastructure and other relevant areas on cybersecurity;

(f) risk assessment including threat, vulnerability, consequence and mitigation; and

(g) emerging technologies.

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

Baseline security for critical information infrastructure.

31. (1) An owner of a designated 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 risks associated with 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) address data protection concerns of the designated critical information infrastructure, consistent with the provisions of the Data Protection Act, 2019;

No. 24 of 2019.

(b) implement and comply with the directives issued under regulation 20; and

(c) appoint or designate a Chief Information Security Officer in accordance with the requirements of regulation 32.

(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) identification, classification and cataloguing of all critical information infrastructure assets;

(b) regulating 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 background checks on all personnel handling critical information infrastructure information or data in the designated critical information infrastructure;

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

(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 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 20;

(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 exercises and drills, in collaboration with the Committee and other critical

information infrastructure sectors for the purposes of verifying readiness of the owner of designated critical information infrastructure in responding to cybersecurity incidents; and

(n) adopting relevant cybersecurity best practices, frameworks and standards, approved by the Committee.

Designation of the Chief Information Security Officer.

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

(2) Without prejudice to paragraph (1), owners of critical information infrastructure may jointly 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) analysing 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 Centre, Sector Cybersecurity Operations Centres and other relevant stakeholders 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) assisting in detection, identification, prevention, response, and recovery measures for cyber threats, risks or incidence in the organization; and

(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.

Qualifications of the Chief Information Security Officer

33. A person shall be qualified as a Chief Information Security Officer if the person—

(a) holds a master's degree in information security, computer science, information technology or a related field;

(b) holds a bachelor's degree from a recognized university;

(c) is a citizen of Kenya;

(d) has at least five years of demonstrable professional experience in the protection of critical information infrastructure;

(e) has demonstrable technical skills, competencies and knowledge on critical information infrastructure audit; and

(f) satisfies the requirements of Chapter Six of the Constitution.

Mandatory requirements.

34. (1) An owner of a critical information infrastructure shall within six months from the date of commencement of these Regulations, formulate, review and update on an annual basis organizational policies, procedures and codes of practice to ensure the 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 procedures;

(b) modalities for—

(i) sharing of critical information infrastructure system or data within the organization;

(ii) transfer of critical information infrastructure system or data to third parties; and

(iii) 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 tests for software against the defined organizational cybersecurity requirements;

(d) securing integration between software components; or

(e) conducting a configurations' review, secure configuration and hardening and patching before deployment of software products.

(4) Where an owner of a critical information infrastructure intends to change the management or make any material change to the

critical information infrastructure's projects, software and their application, the owner shall undertake—

(a) vulnerability assessment and remediation; and

(b) conduct a configurations' review, secure configuration and harden and patch prior to making the changes or going live for technology projects.

Mandatory requirements for licenced operators of international or national internet gateways.

35. (1) Pursuant to section 6(1)(f) of the Act, and upon the commencement of these Regulations, the Committee shall require a licensed operator of an international or the national internet gateway to comply with the cybersecurity standards provided under these Regulations.

(2) A licensed operator of an international or the national gateway, shall upon request by the Committee, submit a safety standards compliance report within thirty days of such request.

(3) In the event there is any internet traffic congestion or suspicious activity, the operator of an international or the national internet gateway shall immediately report to the Committee concerning the connection status of the congested route specifying the causes and solutions for the congestion.

(4) A licensed operator of an international or the national internet gateway shall, upon request by the Committee, prepare, maintain and submit to the Committee technical records, internet portal address allocation records, and route identification of traffic, transiting through the national internet gateway.

(5) Where the operator of an international or the national internet gateway fails to comply to this regulation, the Committee shall in consultation with the sector Regulator, recommend the restriction, suspension or revocation of the operator's license or take any other action in accordance with the relevant laws.

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 satisfied the required safety standards including safeguards specified under paragraph (2).

(2) In evaluating the adequacy of the 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 and under these Regulations.

Protection and preservation of

37. (1) An owner of critical information infrastructure shall implement appropriate safeguards and measures to ensure security of

the premises and surrounding areas in which a critical information infrastructure is situated.

premises and surrounding areas.

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

(a) systems being maintained in a secure place and preventing unauthorized access of such systems, and considering the nature of the database activity and the sensitivity of information therein;

(b) where applicable, sufficient cooling mechanisms to prevent overheating of equipment;

(c) backup equipment to prevent or mitigate the effect of a fluctuation of an electric load;

(d) taking such actions or 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 inside and outside the database systems;

(e) ensuring 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) securing 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 authorized 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 a visitor management system or record keeping system specifying 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 climate control equipment;

(f) installing surveillance cameras at suitable locations for purposes of monitoring the movements and activities within areas hosting a critical information infrastructure;

(g) formulating organizational and operational guidelines to guide the personnel, third parties on the physical or virtual access of the critical information infrastructure; and

(h) undertaking any action necessary to restrict access to a critical information infrastructure.

(4) For purposes of being 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 may 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 scrutiny and examination by either 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 of all critical information infrastructure shall require the person granted access to comply with the conditions for access which may include—

(a) carrying or displaying of the proof of permitted access;

(b) adhering to the restrictions of access to certain parts of the critical infrastructure including restricted access to the personnel within the critical information infrastructure;

(c) complying with the permitted duration of access to the critical information infrastructure; and

(d) monitored access including being escorted while on or in the critical information infrastructure.

(5) An owner of a critical information infrastructure may, at any time, remove any person who has accessed the critical information infrastructure under this regulation, if—

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

(b) access was authorised but 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.

(6) 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 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 analyse 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 their nationality;

(b) reason for accessing the critical information infrastructure;

(c) the duration of the authorization and restrictions applicable to the authorized access of the critical information infrastructure;

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

(e) 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 the Act and these Regulations, 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 distinct of each other and located in a different location from the main location of the critical information infrastructure.

(2) The owner of critical information infrastructure shall ensure that the backup site system—

(a) is stored in a format that permits the retrieval of the information and restoration of a critical information infrastructure system and data in the event of a compromise or destruction of the infrastructure;

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

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

(d) has internal processes that ensures restoration of the critical information in case of a disaster; and

(e) records security incidents 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 where he intends to transfer part or whole of the critical information infrastructure notify the Director in writing.

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

Requirements for an auditor.

44. (1) The Director shall appoint or designate such number of auditors as may be necessary, who shall be responsible for carrying out audit of a critical information infrastructure as 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 the person—

(a) is a citizen of Kenya;

(b) has a degree from a university recognized in Kenya or equivalent;

(c) has at least five years of demonstrable professional experience in the protection of critical information infrastructure;

(d) has demonstrable technical skills, competencies and knowledge on critical information infrastructure audit; and

(e) satisfies the requirements of Chapter Six of the Constitution.

(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) enter a premises to monitor and evaluate the compliance with the directives issued pursuant to these Regulations, upon giving a thirty-day notice to the owner of a critical information infrastructure as contemplated under section 13(2) of the Act; and

(b) require the production of any documents, additional information or any other matter from the owner of a critical information infrastructure relevant to the audit.

Compliance report by owner of critical information infrastructure.

46. (1) Pursuant to section 13 (1) of the Act, the compliance report shall—

(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 satisfy the requirements of the Act and these 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.

(2) 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.

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

(4) Upon consideration of the compliance report under paragraph (2), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the owner of the Critical Information Infrastructure.

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

(6) 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 or an attack that amounts to an attack to a computer or computer system that may result to a cybercrime as contemplated under section 13 (2) of the Act.

(2) For the purposes of this regulation, an imminent threat may include—

(a) evidence of unauthorized access to the critical information infrastructure;

(b) credible intelligence from law enforcement agencies indicating a planned cyber-attack targeting the infrastructure;

(c) an unusual network activity suggesting a potential security breach; or

(d) any other circumstances as may be determined by the Committee.

(3) 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) the 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) the specific documents required to be furnished to the auditor, prior to or during the audit exercise;

(e) the particulars of the auditor assigned to carry out the audit prior to the date of commencement of the audit exercise; and

(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 require the auditor to carry out compliance test to ascertain the adequacy and effectiveness of the controls applied in the critical information infrastructure in order 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) Upon concluding the audit exercise, the auditor shall prepare an audit report which shall contain the following—

(a) summary of the audit findings identified during the audit exercise;

(b) any systemic finding within the critical information infrastructure, which may result in a weakness in the design of a critical information infrastructure;

(c) a recurring finding identified from past audits and that reoccurs irrespective of the recommended corrective action being done; and

(d) recommended good practices in the governance and controls of the critical information infrastructure identified during the audit.

(2) The auditor shall provide recommendations on any of the following areas—

(a) appropriateness of the management's response or proposed actions to the audit finding;

(b) adequacy and effectiveness of the controls put in place by the owner of the critical information infrastructure to mitigate on the identified 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 considering of the audit report submitted under paragraph (2), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the owner of critical information infrastructure.

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

National Public Key Infrastructure components.

51. (1) The National Public Key Infrastructure components comprises—

(a) the Root Certification Authority;

(b) the Certification Authorities;

(c) the Registration Authorities; and

(d) the Subscribers.

(2) 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.

(3) 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.

Root Certification Authority.

52. (1) The Root Certification Authority shall—

(a) establish and maintain the certificate policy and certificate policy statement for the Root Certification Authority;

(b) accredit and audit certification authorities;

(c) issue, renew and revoke licenses to certification authorities;

(d) regulate country to country cross certification and ensure mutual certificate recognition;

(e) regulate certification authorities;

(f) report to the committee at least annually;

(g) inspect the certification authority infrastructure;

(h) develop technical requirements for certification authority infrastructure compliance;

(i) license and accredit certification authorities; and

(j) create awareness and build capacity on the digital certification ecosystem.

Certification Authority.

53. (1) A Certification Authority shall utilize a trustworthy system in performing its services and may be either a public body or a private entity.

(2) A Certification Authority shall generate, manage, issue and distribute public key infrastructure services.

Registration Authority.

54. (1) The Certification Authority may appoint any person or entity 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's information;

(f) transmit the certificate request to Sector Certification Authority

(g) validate certificates by the Certification Authority;

(h) request for revocation, suspension and restoration of certificates; and

(i) ensure that all aspects of registration services and operations are performed.

Subscribers.

55. A subscriber shall obtain a digital certificate from a Certification Authority.

Responsibilities of the Committee on the National Public Key Infrastructure.

56. 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 bi-annual reports from certification authorities; and

(f) create awareness and build capacity on matters relating to the public key.

PART V— CYBERSECURITY CAPABILITY AND CAPACITY

Cybersecurity capabilities.

57. (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-defence 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 organizations 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 National Cybersecurity Academy responsible for meeting the training, research and capacity development needs of the cybersecurity sector and matters related thereto;

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

(f) formulate cybersecurity technical certification standards for organizations.

Training Guide.

58. (1) The Committee, shall formulate and periodically review the 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 Ministries, State Departments, National Government Administration Officers, county departments, agencies 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) recommending 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 Departments, County Departments 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.

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

(a) establishing trusted networks of information sharing partners including administrative guidelines for identifying trusted organizations;

(b) establishing relationships on sharing of cybersecurity information;

(c) providing early warning alerts, announcements and dissemination of information concerning risks and incidents;

(d) sharing information on situational awareness of computer systems vulnerabilities, threats, and incidents in the country and globally;

(e) exploring credible information sharing platforms including encrypted messaging applications, threat intelligence platforms, secure web portals, recommendations on suitable tools based on an organizations size and resources and requirements; and

(f) convening meetings including colloquiums, webinars, seminars, workshops or conferences to share cybersecurity information.

National Cybersecurity Certification Standards.

60. The Committee shall, in consultation with the relevant agencies, formulate National Cybersecurity Certification Standards or recommend adoption of International Cybersecurity Certifications, for purposes of —

(a) attesting compliance of the cybersecurity products, cybersecurity services and cybersecurity processes with the specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data, its functioning or services offered by, or accessible through 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.

61. (1) The Committee shall within twelve months of commencement of these Regulations, develop administrative security automation operational 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 operational 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 standards, reference material, or checklist in creating or enabling continuous monitoring of information security; or

(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.

62. (1) The Committee shall collaborate with the relevant entities including—

(a) public bodies at the national and county governments;

(b) research or training institutions;

(c) private sector entities;

(d) international organizations; or

(e) industry organizations.

(2) The areas of collaboration under paragraph (1) may include—

(a) development of cybercrime and cybersecurity modules of training;

(b) research;

(c) development of standards;

(d) conferences;

(e) workshops;

(f) policy development; or

(g) any other relevant areas.

Database of certified cybersecurity institutions and professionals.

63. The Committee shall maintain an up-to-date database of certified cybersecurity institutions and professionals in Kenya.

PART VI—CYBER THREATS REPORTING

Objectives of reporting of cyber threats.

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

(a) provide actionable information or complaints which may form a basis for investigations and prosecutions;

(b) identify cybercrime threats on citizens and organizations, including 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.

Incident reporting for critical information infrastructure.

65. 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; and

(c) report all cybersecurity incidents to the relevant Sectoral Cybersecurity Operations Centre within twenty-four hours of becoming aware of an incident pursuant to section 40 of Act;

Reporting of cyber threats to the Committee.

66. (1) Pursuant to 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) email addresses;

(ii) official websites

(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 and malicious social media accounts; or

(ix) any other evidence.

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

Establishment of cybercrimes desk. No. 11a of 2011

67. (1) Pursuant to section 40 of the Act and section 24 of the National Police Service Act, 2011, the National Police Service shall, within twelve months of coming into force of these Regulations, establish cybercrimes desk at every police station and police post with appropriately trained personnel from amongst its members.

(2) The officers at the cybercrimes desk shall be responsible for receiving, assessing, acting and where applicable escalating incidents and cyber threats reported by individuals or organizations within its jurisdiction in Form CMCA 7 set out in the Third Schedule.

(3) For purposes of this regulation, the cybercrimes desk shall be both physical at the police stations and police posts and virtual to allow real time reporting of incidents and threats.

Cybercrimes desk personnel training and qualifications.

68. (1) The personnel deployed to the cybercrimes desk contemplated under regulation 67 shall undergo specialized training in cybersecurity and digital forensics to enable them effectively respond to cyber threats or incidents.

(2) Without prejudice to paragraph (1), the Committee may recommend to the National Police Service suitable specialized training programs and collaborate with relevant cybersecurity authorities and organizations in the provision of the training opportunities.

(3) The Committee shall, upon request provide, technical support including advising National Government Administration Officers with relevant cybersecurity awareness and training for effective collaboration on the provisions established under regulation 66 and 67.

Public awareness and reporting.

69. (1) The Committee and the National Police Service shall conduct public awareness campaigns to educate citizens and organizations on the role of cybersecurity desk and the mode of reporting cyber incidents.

(2) The Committee shall, in collaboration with the National Police Service, establish a mechanism for individuals and organizations to report cyber incidents to the nearest police station or police post.

Anonymous reporting of cyber threats.

70. (1) The Committee or any law enforcement agencies, or an organization, shall provide platforms for anonymous reporting to allow any person to disclose useful information relating 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;

(e) an 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 chargeable under section 22 of the Act.

PART VII—MISCELLANEOUS PROVISIONS

Adoption of best practice standards.

71. (1) The Director shall periodically identify and evaluate global cybersecurity best practices and standards and recommend for adoption by the Committee.

(2) The Committee may formulate administrative Standard Operating Procedures based on the recommendations contemplated under paragraph (1) which shall be applicable to the various sectors including owners of critical information infrastructure.

(3) Despite paragraph (2), owners of critical information infrastructure may on their own initiative identify, evaluate and adopt global best practices and operational 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 provided 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 mechanisms.

73. (1) The Committee may on its own motion or by application of an owner of a critical information infrastructure, review any decision made under these Regulations on 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.

(2) 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 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 members and non-members

(1) Each individual members of the Committee shall attend and participate in the meetings of the Committee;

(2) 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(1)(a))

CRITICAL INFORMATION INFRASTRUCTURE SECTORS

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

	Critical Sector	*Critical Subsecto*	*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	(a) Water storage (b) Water Distribution (c) 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 Safe		(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.23(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 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 the market of the Republic; and

(e) adverse and severe effect of the Security of the

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.26(3),27(1)&(3))

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.28(2))

APPLICATION FOR CHANGES IN THE 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	
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.47(3))

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.66(1)&67(2))

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: user	☐ The impacted user		☐ Reporting on behalf of the impacted		
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 8th February, 2024.

KITHURE KINDIKI,
Cabinet Secretary Interior Administration.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI