A green and red tree with text

Description automatically generated

Low view of a building with a balcony

Description automatically generated

SECURITY AND EMERGENCY SERVICES POLICY AND PROCEDURE MANUAL

**SEPTEMBER 2023**

**KONZA TECHNOPOLIS DEVELOPMENT AUTHORITY**

# **SECURITY AND EMERGENCY SERVICES MANAGEMENT POLICY REVIEW SHEET**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue/Revision No | Subject of Amendment | Reviewed By | Authorized By | Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **DEFINITION OF TERMS.**

**Access rights**: Specific rights or actions that are granted to individuals, groups, or entities to gain entry or access to specific physical spaces, assets, or resources within Konza Technopolis.

**Access control**: Measures and practices implemented to regulate and manage the entry, exit, and movement of individuals within Konza Technopolis.

#### **Accountability**:The act of holding an individual answerable for their actions.

**Assurance**:A security assurance can be defined as the confidence that a system meets its security requirements and is resilient against security vulnerabilities and failures.

**Authority**:The body entrusted with the power to determine, adjudicate or control access

**Barrier sensors**: Used to monitor physical barriers such as fence, walls, roofs and windows.

**Biometric reader**: A device that gathers and analyzes biometric features.

**Biometrics**:In access control, the use of a person’s physical characteristics, such as fingerprint or iris pattern, to authenticate identity.

**Breach of security**:A security breach is any incident that results in unauthorized access of premises, data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

#### **Security audit**: Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.

#### **Confidentiality:** Protection of sensitive or private information from unauthorized disclosure, access, or exposure.

**Crime Prevention Through Environmental Design (CPTED):** A method of improving security through strategic building design, as well as the use of other environmental, organizational, or mechanical tactics.

#### **Document control**: The application of restrictions on the use of a document.  This may also be referred to as policy control.  The use of the word policy here means implementing the controls that the rights owner would like to see imposed on the document so that they can control how it is used by those authorized to use it.

#### **Emergency:** An urgent or pressing situation where immediate action is required to ensure the safety of staff, investors and visitors.

**Emergency Services Personnel:** Persons responsible for ensuring public safety and mitigating activities in an emergency (e.g. law enforcement, fire departments, emergency medical services, rescue services).

**Evacuation site:** The designated off-site location where shelter is obtained during an emergency. The evacuation site is used when it is deemed unsafe to be at or return to the residential places and offices within the Technopolis.

**Incident**: An event, occurrence or action that may negatively affect Konza Technopolis operations.

**Investigation**: Is a process of searching, conducting interviews, interrogations, evidence collection and preservation with a view of identification, locating and establishing facts.

**Incident management**: The process of responding to an emergency event or reports of suspicious activity.

**Intrusion detection device**: Technology that uses sensors to detect potential or actual physical security breaches.

**Occurrence Book/platform:** Is a book (Platform) used to record all security incidents.

**Risk**: An event that could cause harm or loss or affect the ability to achieve an objective.

**Perimeter security**: The concept of providing protection of a facility’s outermost boundary.

**Physical security:** Denotes the measures that are designed to deny unauthorized access/intrusion to Technopolis facilities, resources and to protect personnel and property from damage or interference through espionage, theft, vandalism or terrorist attacks. The measures are also intended to prevent the escape of law breakers and culprits of security breaches.

**Scene -** A scene of crime is the physical location where an incident has taken places.

[**Video surveillance:**](http://www.ingrammicroadvisor.com/physical-security/are-you-ready-for-todays-video-surveillance) An electronic surveillance system that records video and sends footage to monitors for viewing and recorders for storage. Includes both closed-circuit television (CCTV) and network-based video systems.

# **LIST OF ABBREVIATIONS**

The following terms are explained as used in this policy.

**AP** - Administration Police

**CCTV**  - Closed Circuit Television

**CEO** - Chief Executive Officer

**CPTED** - Crime Prevention Through Environment Design

**DC**  - Data Centre

**DCI**  - Directorate of Criminal Investigation

**HR** - Human Resource

**ICT** - Information and Communication Technology

**KT**  - Konza Technopolis

**KOTDA** - Konza Technopolis Development Authority

**KWS** - Kenya Wildlife Service

**NIS** - National Intelligence Service

**OSH** - Occupational Safety and Health

**SO**  - Security Officer

**VIP** - Very Important Person

**STI**  - Science Technology and Innovation

# **FOREWORD**

The Management of Konza Technopolis Development Authority places significant importance on the security policy, particularly within the context of our role as a technology-driven organization dedicated to serving Kenyan citizens and playing a central role in the development of Konza Technopolis.

This policy serves as a guiding framework for implementing standard operating procedures and ensuring compliance with legal and regulatory requirements. To set the standards of practice outlined in this Code, this document takes into account the Authority's Vision, Mission, Values, and Mandates. Furthermore, it incorporates the statutory provisions of various acts, including The Survey Act, The Land Act, The Public Participation Bill, The Public Officer Ethics Act 2003, The Civil Service Code of Regulations Revised 2006, The Public Service Commission Act Cap 7 85, The Anti-Corruption and Economic Crimes Act 2003, and other relevant regulations.

We call upon our dedicated staff, stakeholders, investors, development partners, and the community at large to join hands in supporting the Authority by adhering to this Policy. Should anyone come across any instances of unethical practice, we urge you to promptly report it to the Authority. Together, we can ensure the continued success and integrity of Konza Technopolis.

Signed

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

John Paul Okwiri

**CHIEF EXECUTIVE OFFICER**

**TABLE OF CONTENTS**

[SECURITY AND EMERGENCY SERVICES MANAGEMENT POLICY REVIEW SHEET 1](#_Toc147227108)

[DEFINITION OF TERMS. 2](#_Toc147227109)

[LIST OF ABBREVIATIONS 5](#_Toc147227110)

[FOREWORD 6](#_Toc147227111)

[KONZA TECHNOPOLIS IDENTITY 9](#_Toc147227112)

[1.0 INTRODUCTION 9](#_Toc147227113)

[1.1 Vision 9](#_Toc147227114)

[1.2 Mission 9](#_Toc147227115)

[1.3 Mandate 9](#_Toc147227116)

[1.4 Core Values 9](#_Toc147227117)

[1.5 Strategic Objectives: 9](#_Toc147227118)

[1.6 Project background 10](#_Toc147227119)

[2.0 PREAMBLE. 11](#_Toc147227120)

[2.1 Policy Statement. 11](#_Toc147227121)

[2.2 Objectives of the policy. 11](#_Toc147227122)

[2.3 Legal Framework. 12](#_Toc147227123)

[2.4 The scope of the policy. 12](#_Toc147227124)

[2.5 Policy Communication. 12](#_Toc147227125)

[2.6 Privacy and Responsibility. 12](#_Toc147227126)

[3.0 PHYSICAL SECURITY PROTECTION 13](#_Toc147227127)

[3.1 Access control. 13](#_Toc147227128)

[3.2 Perimeter protection. 13](#_Toc147227129)

[3.2.5 Close Circuit Television (CCTV). 14](#_Toc147227130)

[3.3 Security at Construction sites. 14](#_Toc147227131)

[3.4 Buildings Security. 14](#_Toc147227132)

[3.5 Clear desk and clear screen requirement. 15](#_Toc147227133)

[3.6 Identification of staff and visitors. 15](#_Toc147227134)

[4.0 INCIDENT REPORTING AND INVESTIGATIONS. 16](#_Toc147227135)

[4.1 Incident Reporting. 16](#_Toc147227136)

[4.2 Scene of crime management. 16](#_Toc147227137)

[4.3 Investigation. 16](#_Toc147227138)

[4.4 Lost and found property. 16](#_Toc147227139)

[5.0 EMERGENCY AND INCIDENT RESPONSE. 18](#_Toc147227140)

[5.1 Incident response team. 18](#_Toc147227141)

[5.2 Emergency Situations. 18](#_Toc147227142)

[5.3 False Fire Alarms. 19](#_Toc147227143)

[6.0 POLICY MANAGEMENT AND IMPLEMENTATION. 20](#_Toc147227144)

[6.1 Policy management. 20](#_Toc147227145)

[6.2 Policy implementation. 20](#_Toc147227146)

[6.3 Security committee. 20](#_Toc147227147)

[6.4 Departmental head in charge of security and emergency services 21](#_Toc147227148)

[6.4.1 Role of Security Officers. 21](#_Toc147227149)

[6.4.2 Police Officers. 22](#_Toc147227150)

[6.4.3 Roles of security guards. 22](#_Toc147227151)

[7.0 PRIVATE SECURITY SERVICES PROVIDERS. 24](#_Toc147227152)

[7.1 Contractual Obligation of Private Security Providers. 24](#_Toc147227153)

[7.2 Subcontracting. 24](#_Toc147227154)

[7.3 Handing Over and Taking Over of Assignment. 24](#_Toc147227155)

[8.0 SECURITY QUALITY ASSURANCE. 26](#_Toc147227156)

[8.1 Quality Assurance and Control. 26](#_Toc147227157)

[8.2 Security Risk Analysis. 26](#_Toc147227158)

[8.3 Security Audit. 27](#_Toc147227159)

[8.4 Security Surveys. 28](#_Toc147227160)

[8.5 Security Tests. 28](#_Toc147227161)

[8.6 Policy test and qualities. 29](#_Toc147227162)

[9.0 Policy Review date 30](#_Toc147227163)

[10.0 Policy effective date 30](#_Toc147227164)

# **KONZA TECHNOPOLIS IDENTITY**

# **1.0 INTRODUCTION**

## **1.1 Vision**

A leading global Technopolis and innovation hub.

## **1.2 Mission**

To develop a thriving sustainable smart city and a vibrant innovation ecosystem contributing to Kenya’s knowledge economy.

## **1.3 Mandate**

The mandate of KoTDA is to develop Konza Technopolis as a globally competitive smart city by creating an enabling environment through utilization of ICT for socio-economic development.

## **1.4 Core Values**

1. Nurturing
2. Innovation
3. Collaboration
4. Excellence

## **1.5 Strategic Objectives:**

1. Develop and manage a world-class smart city with a vibrant, safe, secure, healthy and sustainable ecosystem.
2. Form partnerships with other actors in the National Innovation System, to recruit, attract, and develop high-end talent as well as create relevant, and smart innovative solutions and commercialize them.
3. Mobilize adequate and sustainable funding to meet the Authority’s mandate and changing needs of the business community and residents.
4. Create a strong brand and image of Konza Technopolis that will attract, facilitate, and retain investors.
5. Ensure that the Authority has adequate institutional capacity to fulfil its mandate.

## **1.6 Project background**

Konza Technopolis (KT) is envisioned to be a sustainable, world-class technology hub and a major economic driver for Kenya, with a vibrant mix of businesses, workers, residents, and urban amenities. KT will create high value jobs, boost the country’s GDP by focusing on Research, Development and Entrepreneurship in the Science Technology and Innovation (STI) sector. This will position Kenya as a global center for innovation and Africa’s technology hub.

Konza Technopolis aims to attract Research, Education and Commercial partners in Information Technology Enabled Services (ITES), Life Sciences and Engineering. Increased innovation will lead to an increase in patenting and increased quality will produce skilled workforce for industries. KT will attract investors and build programs aimed at commercializing the products of research. It will provide a good innovation ecosystem to educate new and existing technology entrepreneurs and for multinational companies entering Africa to consider setting up their offices or branches.

Konza Technopolis will be a 'smart city' with highly advanced overall infrastructure, sustainable developments, communication networks and market viability. KT will feature world-class civic and commercial architecture and it will be a Regional Innovation Hub; KT will also host a high-quality Technology University, Smart Schools, Research Labs, Recreational Facilities (Sports Stadium, Film and Media Centre), Hospitality (Hotels and Convention Centers), Smart City Solutions (Smart Traffic, Smart Parking and Smart Governance) and world-class infrastructure.

Konza Technopolis requires a comprehensive security policy to ensure safe and secure environment that meets all security standards, framework for all developments to achieve its envisioned status of a smart and sustainable city.

# **2.0 PREAMBLE**.

An effective physical security management policy is key to Konza Technopolis success. The evolving security threats targeting critical infrastructure necessitates the formulation of this policy aimed at deterring and suppressing criminal activities at Technopolis.

This policy outlines security standards, procedures and provides guidelines on the administration of security operations. This policy will be modified and amended to fit the Technopolis security needs as they evolve.

## **2.1 Policy Statement.**

The Authority is dedicated in creating and maintaining an efficient, sustainable, and secure environment as a value addition for its residents, businesses, and visitors. As part of the commitment, this policy outlines Konza Technopolis’ principles, objectives, and guidelines for the implementation and management of security and emergency services.

## **2.2 Objectives of the policy.**

The objectives of the emergency and security services management policy are to:

1. Ensure that all persons permitted to access the Technopolis premises are aware of and fully comply with relevant legislation as described in this and other policies.
2. Introduce a consistent approach to security, ensuring that all stakeholders fully understand their own responsibilities.
3. Expedite the delivery of life-saving assistance by triggering appropriate incident response and establish simplified procedures of handling emergencies.
4. Create and maintain within the Authority a level of awareness of the need for security as an integral part of day-to-day business.
5. Develop a business continuity and business recovery plan.
6. Protecting life and all assets under the Technopolis.

## **2.3 Legal Framework.**

The policy is intended to work in conjunction with the Kenyan Constitution and other existing affiliated policies on;

1. Private Security Regulation Act, 2016.
2. KoTDA Human Resource Policy and Procedure Manual
3. KoTDA ICT Policy
4. Occupation safety and health Act, 2007
5. Criminal Procedure Code
6. KoTDA Risk Management Policy.

## **2.4 The scope of the policy.**

This policy applies to all Konza Technopolis facilities and assets including employees, trainees, investors, contractors, customers, information, vehicles, offices, visitors, workshops, goods on transit and other items/facilities required for operational and administrative purposes. All KoTDA operations and processes are covered.

## **2.5 Policy Communication.**

It is the responsibility of the departmental head of security and emergency services to ensure this policy, and any subsequent updates, are communicated to sensitize the public about any actions they should undertake to ensure compliance with this policy.

Methods of disseminating this information include: town hall meetings, emails, signage informing the public of sensitive/restricted areas and surveillance areas within the Technopolis.

## **2.6 Privacy and Responsibility.**

This policy is considered “confidential” and will be made available to the concerned persons with proper document access control protocols. Subsequent changes and versions of this document shall be controlled.

The responsibility for the implementation of this policy rests with the departmental head of function.

# **3.0 PHYSICAL SECURITY PROTECTION**

This involves the deployment of multi-agency security management approaches and systems i.e. protective barriers, security guards, police officers and artificial intelligence.

## **3.1 Access control.**

The Authority shall utilize technologies, procedures, databases and staff to realize this objective. In realization of this objective, the Authority shall deploy a hybrid access control system. Access control to the Technopolis shall be guided by an approved access control procedure.

## **3.2 Perimeter protection****.**

**3.2.1 Crime Prevention Through Environmental Design.**

The Authority shall leverage on environmental factors to reduce opportunities for crime and enhance safety and security within the Technopolis. The following environmental factors shall be considered to bolster perimeter protection;

Lighting: The Authority should ensure that the city is well-lit to reduce hiding places for potential criminals, increase visibility and create a sense of comfort and safety. This method emphasizes the use of lighting to ensure that critical areas, walkways, entrances, and parking lots are well illuminated. Motion sensor lights should be installed at vital installations to deter intruders.

Landscaping: The Authority has adopted the use of undulating bumps that mimic the surrounding natural landscape to promote natural surveillance, deter criminal activities, and create a welcoming environment.

Community Engagement: For the safety of the city, the Authority recognizes the importance of community engagement and involvement. The Security section shall liaise with residents, employees, and stakeholders such as NGAO to actively participate in security initiatives and foster a sense of collective responsibility and inclusivity in management of security at the Technopolis.

**3.2.2 Physical barriers.**

Barriers, gates and bollards shall serve as the outermost layer of physical security that protects Konza Technopolis against unauthorized access, intrusions, and potential threats.

**3.2.3 Intrusion detection and alarm systems.**

Intrusion detection systems shall be adopted to assess, deter threats and improve incident analysis. The intrusion detection systems shall be integrated with [alarm systems](https://en.wikipedia.org/wiki/Alarm_systems) and sensors to alert security personnel of breaching attempts.

### 3.2.5 Close Circuit Television (CCTV).

CCTV allows camera images to be recorded, monitor and retrieved to maintain visual surveillance of vital installations at the Technopolis. The Authority shall integrate all standalone intelligence surveillance systems to allow for real time monitoring and emergency response. The Authority will establish a control room and furnish it with the necessary resources, enabling it to function as an efficient conduit for conveying security intelligence information to the city security teams. An effective CCTV system shall assist the security section to reconstruct security breaches at all facilities and outdoor areas, as well as to identify those involved in the incident. The policy is supported by the CCTV Procedures which detail the collection and use, further including the requirement to restrict access to protect personal information collected. All CCTV recordings will be stored for a period of 90 days. The departmental head of function in liaison with Manager ICT and Smart City Solutions will undertake annual evaluations of the CCTV system to ensure overall compliance with this policy.

## **3.3 Security at Construction sites.**

Construction sites security shall be prioritized. All contractors working at Konza Technopolis have a general responsibility for their site security and are expected to report all security incidences to KoTDA departmental head in charge of security and emergency services for continuous monitoring. Although each construction site will present unique situations and risks, the security section shall develop and review construction site security best practices that will be implemented in conjunction with this policy.

## **3.4 Buildings Security.**

Office physical security involves implementing measures to protect the physical assets, personnel, and sensitive information within an office environment. Konza Technopolis being a business destination, this policy requires various tenants take responsibility for the security of their offices and buildings. Further, this policy shall be implemented together with KoTDA access control procedure which provides guidelines on the best office security practices to guarantee safety of each premise.

Intrusion detection systems shall be deployed in vital installations to detect, deter, delay and respond to security breaches.

## **3.5 Clear desk and clear screen requirement.**

The Authority requires all staff to ensure that they maintain a clean and organized workplace whenever they are out of the office either on leave or during non-working hours. The guidelines are essential for enhancing documents security, reducing the risk of information security and promoting a professional and organized work environment.

Staff shall be expected to clear their workspaces, secure storage areas by ensuring that sensitive documents are locked away, electronic devices such as computers should be locked or logged out when not in use, ensure confidential information is kept away from unauthorized persons and proper disposal of sensitive data.

## **3.6** **Identification of staff and visitors.**

The Authority staff shall be required to display their staff identification card while within the Technopolis precincts. The Authority staff card shall bear the name of the staff, staff personal number, national identification card and position held. Interns and attachees shall be issued with temporary staff cards. Visitors shall provide their identification documents, booked and issued with visitor's badge prior to granting access to vital installations.

# **4.0 INCIDENT REPORTING AND INVESTIGATIONS.**

## **4.1 Incident Reporting.**

All security incidents, breaches, or suspicious activities should be promptly reported to the security team. These incidents include Injuries, property damage, and near misses. Employees, contractors, and visitors have a personal responsibility to report any observed or suspected incidents. Reporting incidences aids

in the recording, tracking occurrences, management and improvement of preventative actions. Incidents shall invite positive reaction, including investigation of the circumstances, systematic recording of the incidents and designing remedial measures. To ensure incidents are effectively handled at the Technopolis, the security section has formulated incident reporting procedure which shall be applied in conjunction with this policy.

## **4.2 Scene of crime management.**

The primary goal of crime scene management is to preserve, collect, document, and analyze physical evidence and information in a way that maintains the integrity of the scene and ensures a thorough investigation. This process is critical in securing accurate and reliable evidence to be used in court and leads to successful case resolutions. All scenes of crime at the Technopolis shall be protected and safeguarded in line with crime scene management guidelines.

## **4.3 Investigation.**

Security incident investigations shall be caried out to identify, analyze and resolve security incidents occurring at Konza Technopolis. Immediately an incident is reported, the departmental head in charge of security and emergency services shall ensure preliminary incident report recorded. The preliminary incident findings shall guide the next course of action. All staff and visitors are required to cooperate with investigations when requested to do so. Investigations at the Technopolis shall be carried out as per the established investigation guidelines.

The Authority shall liaise with the state security agencies to ensure that all reported cases are pursued to the end.

## **4.4 Lost and found property.**

Documentation of these guidelines ensures a systematic and transparent approach to managing lost and found property within the Technopolis, promoting accountability and efficient resolution for both owners and finders of lost items. Under this section, security teams shall design a lost and found property form to enable staff, visitors and contractors to complete their own Lost Property Reports. Disposal and identification of the rightful owner shall be carried out as stipulated in the lost and found procedure.

# **5.0 EMERGENCY AND INCIDENT RESPONSE.**

The emergency and incident response section provides information to assist in the development of workplace emergency preparedness and response programs. All stakeholders working within Konza Technopolis should have an emergency response plan in place. Customers and stakeholders expect it as an indication of reliable business operation.

## **5.1 Incident response team.**

The departmental head in charge of security and emergency services shall establish an incident response team comprising of security officers, police officers, guards and trained fire and safety marshals. These members shall be trained and designated to respond to incidents that occur within the Technopolis. The emergency and incident response team shall carry out their mandate as guided by the Emergency and incident response procedure and report as per the security incident form.

All Staff, Visitors and contractors are encouraged to familiarize themselves with the information provided by the OSHA on their expectations during emergencies. They should also acquaint themselves with the contact details of security team, emergency and incident response team and police officers to report and communicate emergency incidents.

## **5.2 Emergency Situations.**

All emergency rescues shall be conducted in accordance with the Security Act Cap 57. In the event of an emergency, the departmental head in charge of security and emergency services shall ensure the following actions have been initiated;

Immediate Response: Quickly initiate an appropriate emergency response plan, which might involve sounding alarms, notifying emergency services, and alerting both the staff and public.

Communication: Establish clear communication channels to disseminate information to those affected, emergency responders, and relevant stakeholders. Communication shall be accurate, timely, and transparent.

Evacuation: If necessary, initiate an evacuation plan to move people away from danger. Evacuation routes and assembly points should be clearly marked and communicated to all occupants. Evacuation at the Technopolis shall be guided by the Authority’s evacuation procedure.

First Aid and Medical Assistance: Provide immediate medical attention to those injured or in need. Trained personnel should administer first aid, and emergency medical services such as ambulances should be contacted for more serious injuries.

Accountability: Maintain a record of individuals on the premises to ensure that everyone is accounted for and no one is left behind.

Emergency Services Coordination: Collaborate with emergency services such as fire departments, police, medical teams, and other relevant agencies to coordinate efforts and resources effectively.

Containment: If the emergency involves hazardous materials, take steps to contain and mitigate the impact of these substances to prevent further harm.

Communication Updates: Continuously update affected individuals and stakeholders about the evolving situation, instructions, and any changes to the response plan.

Support and Comfort: Provide psychological support to affected individuals and offer a safe and supportive environment for them during and after the emergency.

Assessment and Review: After the situation is under control, conduct a thorough assessment of the emergency response to identify strengths, weaknesses, and areas for improvement. Use this information to update and enhance emergency plans.

Learning and Training: Regularly conduct emergency drills and training exercises for staff and occupants to ensure they are familiar with emergency procedures and can respond effectively.

Documentation: Maintain accurate records of the emergency, including actions taken, communication exchanges, and outcomes. These records can be invaluable for post-incident analysis and reporting.

Debrief and continuous communication, as required, to the Authority’s staff, the general public, and the media.

## **5.3 False Fire Alarms.**

Fire alarms are a life safety system and should only be activated in the event of a fire or during authorized fire drills. Therefore, Police and Security Officers will pursue all available legal actions against anyone who willfully creates a false alarm of fire.

# **6.0 POLICY MANAGEMENT AND IMPLEMENTATION.**

## **6.1 Policy management.**

For the Authority to meet its safety and security needs, the security services have been organized into an internal Security management team, Police Officers and outsourced private security firms. The Authority also engages other government and private security agencies such as NIS, DCI and KWS to achieve the desired security objectives.

## **6.2 Policy implementation.**

This policy shall be implemented by the CEO through the departmental head in charge of security and emergency services. It is the responsibility of the departmental head in charge of security and emergency services to ensure compliance and implementation of this policy.

## **6.3 Security committee.**

The Authority’s Chief Executive Officer shall appoint a security and emergency services committee comprising of representatives from various departments to carry out the following responsibilities.

1. Advice Konza Technopolis stakeholders on security measures necessary for their operations within Konza Technopolis.
2. Conduct regular risk assessments to identify and evaluate potential security threats and vulnerabilities within Konza Technopolis.
3. Develop, review, and update security policies, procedures, and guidelines to ensure they are current and aligned with industry best practices and regulatory requirements.
4. Formulate and implement a comprehensive security strategy that outlines the Authorities security goals, objectives, and priorities.
5. Develop and maintain an incident response plan to address security incidents, breaches, and emergencies effectively.
6. Monitor and ensure compliance with applicable security laws, regulations, industry standards, and contractual obligations.
7. Promote security awareness among employees and provide training programs to enhance their understanding of security risks and best practices.
8. Assess and recommend security technologies, tools, and solutions to protect the organization's infrastructure, data, and assets.
9. Analyze security incidents and breaches to determine their root causes and lessons learned.

## **6.4 Departmental head in charge of security and emergency services**

The departmental head of security and emergency services will be the overall in charge and shall:

1. In liaison with the Manager Finance & Accounts budget for operational funds for institutional support which includes adequate funding for security operations and emergency services.
2. Create awareness amongst Authority staff on the importance of this policy and their responsibilities.
3. Regularly monitor the policy to determine its practicability.

## **6.4.1 Role of Security Officers.**

SO shall be responsible for developing, coordinating and implementing the Authority’s security strategies, policies and standards for protection and preservation of the KT assets to achieve KoTDA’s mandate.

Functions.

1. Developing, implementing and monitoring security strategies, policies and standards in line with the Konza Technopolis mission and vision.
2. Liaising with national security agencies to ensure security of Authority's assets and business operations.
3. Overseeing Incident, Emergency Response Plan and investigations into security breaches against the Authority premises.
4. Managing, training and monitoring outsourced security service providers to meet KT security objectives and enhance their performance.
5. Maintaining an up-to-date databank of security incidents and trends and reporting them for management information and action.
6. Advising the Authority on security-related matters affecting its operations.
7. Sensitization of staff residents and guest on security policy and procedures.
8. Testing security and surveillance systems during installation and on regular basis to ensure their effectiveness.
9. Put in place preventive measures and deal expeditiously with security breaches that may occur at KT in liaison with police and security systems.
10. Allocate/assign duties to security teams.
11. Provide emergency response services.
12. Conduct regular security spot checks within KT.

## **6.4.2 Police Officers.**

Police Officers functions shall be specifically aligned to the security and emergency operations at Konza Technopolis. The officers shall;

1. Police officers will conduct their roles in accordance with the National Police Service Act, 2011.
2. Prevent and detect crimes.
3. Ensure safety and security of Konza Technopolis properties and assets.
4. Investigate offences at Konza Technopolis and present detailed report on the findings and actions taken regarding the offence.
5. Provide escort duties to dignitaries as advised by Officer in charge of security.
6. Coordinate with DCI and other security agencies, county security committees and community policing initiative committees to safeguard KT properties.
7. Provide public safety and security to Authority’s employees, stakeholders and members of public.
8. Conduct regular and impromptu patrols at KT.
9. Enforce rules and regulations related to Authority’s operations.
10. Guard Konza Complex, Data Centers (DC) and all other vital installations.
11. Provide monthly security reports on their operations at KT to the Authority Management.

## **6.4.3 Roles of security guards.**

1. To ensure they are visible within their jurisdictions of operations.
2. Guards stationed at entrances of buildings will manage access control by authorizing or denying entrance.
3. Secure Authority’s premises and personnel by patrolling property, monitoring surveillance equipment, inspecting buildings and access points.
4. Ensure the security, safety and well-being of all staff, visitors and premises.
5. Prevent losses and damage by reporting irregularities, informing violators of policy, procedure and detaining trespassers.
6. Protect Authority Assets from theft, assault, fire, burglary, vandalism and any other safety issues.
7. To sense a crisis brewing and act accordingly to quell the situation.
8. Respond to alarm alerts and react in a timely manner.
9. Compile reports by recording observations, information, occurrences and surveillance activities and interviewing witnesses.
10. Obtain help by sounding alarms in dangerous situations like assault with deadly weapons or armed robbery.
11. To strictly adhere to and implement policies established by the Authority such as standard operation procedures and assignment instructions.
12. Controlling traffic by directing vehicles in accordance with KoTDA Transport policy and The Traffic Act, Cap 403.
13. Provide crowd management at large gatherings within the Technopolis to maintain safety of people and property.

# **7.0 PRIVATE SECURITY SERVICES PROVIDERS.**

## **7.1 Contractual Obligation of Private Security Providers.**

The security firm shall be fully responsible for all work and services performed by its security guards, and shall for this purpose employ qualified, competent, and well-trained guards to perform the services under the Contract.

The security firm shall take all reasonable measures to ensure that their personnel conform to the highest standards of moral and ethical conduct. KoTDA may, at any time, request in writing the withdrawal or replacement of any personnel of the security firm assigned to perform work or services under Contract. The firm shall, at its own cost and expense, withdraw or replace such personnel forthwith. A request by KoTDA for withdrawal or replacement of the personnel shall not be deemed a termination of an existing Contract.

KoTDA shall not be liable for any action, omission, negligence or misconduct of the Contractor's employees, agents, servants, or subcontractors nor for any insurance coverage which may be necessary or desirable for the purpose of an existing, nor for any costs, expenses or claims associated with any illness, injury, death or disability of their employees, agents, servants, or subcontractors performing work or services in connection with an existing contract.

## **7.2 Subcontracting.**

In the event that the main security firm requires the services of subcontractors, the contracted firm shall obtain a prior written approval and clearance of KoTDA for all subcontractors. KoTDA’s approval for a subcontractor shall not relieve the main contractor of any of its obligations as stated in the contract. The terms of any subcontract shall be subject to and conform to the provisions of the Contract.

All security firms must align their operations in accordance with Private Security Regulation Act No. 13 of 2016.

## **7.3 Handing Over and Taking Over of Assignment.**

An existing contract shall be in force for a specified period as determined by KoTDA Security Committee, unless terminated earlier. KoTDA may, at its option, decide to extend the term of an existing Contract. In such case, KoTDA shall provide the contractor with at least thirty (30) days written notice of its intent to exercise this option. Upon termination/expiry of the contract, the two security firms (incoming and outgoing) shall be expected to procedurally hand over and take over assignment for seamless transition of security services.

# **8.0 SECURITY QUALITY ASSURANCE.**

## **8.1 Quality Assurance and Control.**

The purpose of KT security policy is to provide quality assurance guidelines and framework for auditing security and safety operational functions at planned intervals to ensure;

* Compliance with the Security Policy to achieve security objectives.
* Effectiveness of Security controls.
* Monitoring and evaluation of the effectiveness of outsourced security service providers.

The following are security quality assurance standards;

1. The Authority shall provide quality assurance and control guidelines for monitoring and auditing security operational functions to assess their effectiveness.
2. The guidelines shall cover all forms of security protection of the Authority and its stakeholders.
3. The officer in charge of security shall be responsible for implementing quality control measures in accordance with the Security Policy Manual.
4. These measures shall be implemented by means of spot checks, walk-about, surveys, security tests and security audits along with both scheduled and ad-hoc full system vulnerability tests.
5. The officer in charge of security shall take the necessary corrective measures for all non- conformities as and when they are reported.
6. Security surveys, Security tests and other quality assurance and control exercises may involve other departments and functions.

## **8.2 Security Risk Analysis.**

The starting point for understanding the security environment is to evaluate security related risks. This evaluation should be based on:

1. Location and nature of the area.
2. Building construction and design Premises use.
3. Current access control or other security measures.
4. Past security record.
5. Value and desirability of contents.

All departments and divisions will be responsible for assessing and mitigating security related risks arising from their activities. In liaison with the Security office, departments and sections should carry out periodic security risk assessments to determine their security needs.

The security risk analysis should be carried out annually or more frequently if there have been changes to the building or the security environment. Once a risk analysis has been prepared it should be evaluated in consultation with the departmental head of security and emergency services. A decision will be made on the level of exposure to security-related risks and the appropriate measures to deal with the risks.

## **8.3 Security Audit.**

Konza Technopolis shall conduct systematic evaluation of existing security systems and infrastructure to establish compliance with security policies and identify gaps.

1. Security audit reports shall be shared with respective security officers and other departmental heads under review.
2. The audit report shall assess the adequacy and continued effectiveness of security systems, policies, standards and procedures.
3. The audit report shall summarize the following:

* Strengths and weaknesses of the respective areas audited;
* Recommended action from the security auditors.
* Overall management evaluation of the security audit; and
* Performance assessment of the audited areas.

1. The security officers shall regularly review findings and recommendations arising from quality control activities in all installations.
2. The security officers shall determine corrective, preventive and actual implementation of audit recommendations.
3. The officer in charge of security shall be responsible for liaison with all process owners affected by the findings arising from quality control activities and quality assurance audits.

## **8.4 Security Surveys.**

Konza Technopolis security officers shall establish an elaborate process of examining of a facility and its operations with respect to personnel and assets to identify risks, vulnerabilities and threats for purposes of recommending appropriate mitigation measures.

Annual or event driven security surveys shall be conducted to identify needs and weaknesses of the KT security infrastructure.

Depth and scope of the survey shall encompass all features and processes that affect the KT security.

The security surveys shall be conducted:

* To assess and evaluate KT operational environment to determine its security risks and vulnerabilities.
* To examine a specific installation/facility within KT to determine security risks and vulnerabilities; and
* To determine and recommend proactive measures that are commensurate with the threat level.

## **8.5 Security Tests.**

It’s a process of deliberately attempting to breach security systems, policies, standards and procedures in order to assess their effectiveness, identify flaws and vulnerabilities and recommend appropriate corrective measures.

Security tests shall be conducted through the following guidelines:

1. KT Security officers shall conduct security tests to assess the effectiveness and proper implementation of security controls.
2. Security tests shall be conducted regularly, on impromptu basis or in testing a newly installed security system.
3. Such tests may be simulated and carried out covertly by persons to cover a range of security systems and processes. This may be achieved by persons attempting to go through security checks with dummy explosive devices or weapons concealed in their bags to test the existing security measures.
4. Tests shall be carried out adequately and not targeted at intimidating or demoralizing staff.
5. Test results shall not be used to penalize employees who fail to meet expectations but rather as a tool to improve job performance and consequently overall security.
6. The tests for alertness of security personnel shall be conducted with great caution to avoid violent confrontations and injuries or even demotivating such personnel.
7. An effective security testing shall observe the following:

* Conformity with existing laws and regulations.
* Does not jeopardize the safety and security of people and installations.
* Does not lead to damage of KT property; and
* Does not inconvenience the public and persons or organizations not being tested.

1. Security tests may require notification of police authorities and other security agencies where applicable.
2. Security tests shall be conducted by qualified personnel without prior notification to the operating or supervisory personnel (Management, however, may be made aware).
3. Some security tests may require prior authorization for example where dummy weapons may be used or simulations of terrorism attack are involved.
4. Sufficient precautionary measures shall be exercised to prevent overreaction and shock/trauma that could lead to injuries of staff and those involved.

## **8.6 Policy test and qualities.**

The effectiveness of security policy will be determined by:

1. Number of successful/unsuccessful crimes.
2. Number of successful /unsuccessful disruptions.
3. Time between detection, assessment and recovery steps.
4. Business impacts of disruptions.
5. Number of false positive detection alerts.
6. Time to restore operational environments.
7. Financial loss of a successful crime/ disruptions.

# **9.0 Policy Review date**

Once approved this policy will be reviewed as and when needed.

# **10.0 Policy effective date**

This policy comes into effective on the date of approval by the Board of Directors.

Signed

…………………………..…

**John Paul Okwiri**

**CEO – Konza Technopolis Development Authority**