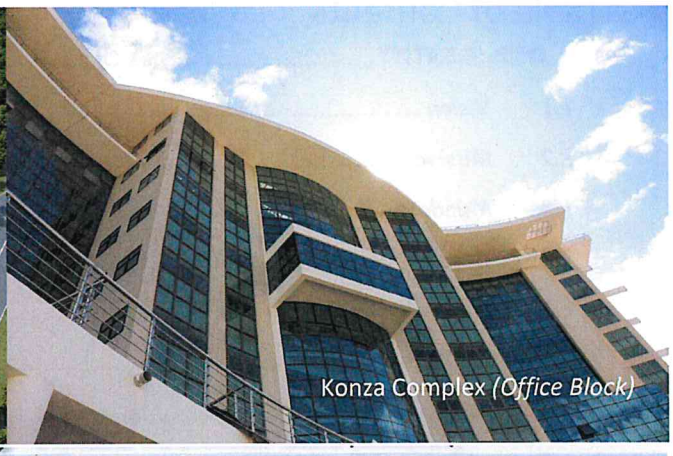
KONZA
Technopolis


Konza National Data Centre & Smart City Facilities


Konza Complex *(Office Block)*


Horizontal Infrastructure through EPC-F

INFORMATION COMMUNICATION TECHNOLOGY POLICY .

KONZA TECHNOPOLIS DEVELOPMENT AUTHORITY

Silicon Savannah

Table of Contents

1 OUR IDENTITY

1.1 Vision

To be a leading global technology and innovation hub.

1.2 Mission

To develop a sustainable smart city and an innovation ecosystem, contributing to Kenya's knowledge-based 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

- Simplicity
- Professionalism
- Passion for excellence
- Agility
- Collaboration

1.5 Strategic Objectives:

- Develop and manage a world-class smart city with a vibrant, safe, and secure, healthy and sustainable ecosystem.
- 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.
- Mobilise adequate and sustainable funding to meet the Authority's mandate and changing needs of the business community and residents.
- Create a strong brand and image of Konza Technopolis that will attract, facilitate, and retain investors.
- Ensure that the Authority has adequate institutional capacity to fulfil its mandate.

Silicon Savannah

FOREWORD

The Management of Konza Technopolis Development Authority recognizes the critical role of ethical service and professionalism in service delivery in addition to concerted efforts from staff as a means to achieve the Authority's Vision, Mission and Mandate.

In order to promote transparency and accountability in the Authority, it is important to define the Authority's standards of practice to regulate behaviours, interactions and actions of its members of staff. The Management recognizes unethical and unprofessional conducts as impediments to social and economic development which also undermines confidence in public institutions.

The KoTDA ICT Policy outlines the standards for the Authority's ICT management. This will ensure that the Authority delivers its services and supports various activities that enhances sustainable development with integrity and without diminishing the Authority's reputation.

To inform the standards of practice stipulated in this Code, this document takes cognizance of the Authority's Vision, Mission, Values and Mandates. It also incorporates the statutory provisions of various acts namely; *The Survey Act , The Land Act 2012, The Public Participation Bill 2018, Public Procurement and Disposal Act 2015, The Public Officer Ethics Act 2003, The Civil Service Code of Regulations Revised 2006,* The *Public Service Commission Act Cap 185, The Anti-Corruption and Economic Crimes Act 2003* and other relevant regulations.

To create a physical environment that fosters corporate innovation for the furtherance of our goal of developing a smart city, it is important to have the free social environment.

I therefore call for a concerted effort from our staff, stakeholders, investors, development partners and the community to support the Authority through adherence to this Policy. Any incidence of unethical practice should be reported to the Authority.

Date: 18/06/24

Eng. John Tanui, MBS

CHIEF EXECUTIVE OFFICER

2 PROJECT BACKGROUND

Konza Technopolis is a smart city designed and implemented by the government of Kenya to enhance Kenya's innovation ecosystem and digital economy by providing the missing infrastructural and technological link.

To bridge the **technological gap** and ensure the city is established to smart city standards as envisaged in the city's *Masterplan*, the *Vision 2030 Blueprint* and the *Kenya's Digital Economy Blueprint – 2019*, the government is implementing the Konza National Data Centre and Smart City Facilities project.

Whereas to bridge the **infrastructural gap** and ensure the city is established to smart city standards as envisaged in the city's *Masterplan*, the *Vision 2030 Blueprint* and the *Kenya's Digital Economy Blueprint – 2019*, the government is implementing the Horizontal Infrastructure project which establishes Phase 1 Roads and Streetscapes, Wastewater Reclamation Facility, Municipal/ Public Buildings and Parks etc.

3 Glossary

KoTDA	-	Konza Technopolis Development Authority
ICT	-	Information Communication Technology
SLA	–	Service Level Agreement
ISO	-	International Organization of Standards
ERP	-	Enterprise Resource Planning

"ICT" in this policy refers to all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are owned, controlled, or operated by KoTDA.

"User" means anyone who operates or interfaces with ICT. It includes KoTDA staff, interns, or any other partner of the Authority.

"Authorized User" means a member of the staff, interns allowed to use ICT resources.

"ICT Assets" means any software, hardware or service resources that are utilized to provide ICT services by the Authority.

4 Preamble

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. KoTDA is not an exception. While the board and the management of KoTDA recognize this fact, organizations all over the world, including KoTDA, are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance. The security threats include computer-assisted fraud, espionage, sabotage, vandalism, fire, or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

The Konza Technopolis ICT Policy provides policies and guidelines for compliance, acceptable and secure use of information communication technology within the Authority that must be followed by all staff. It also provides guidelines upon which the policy shall be administered and the correct procedures to be followed.

The Authority will keep the ICT Policy current and relevant. Therefore, from time to time it will be necessary to modify and amend appropriate sections of this policy or to add new procedures as may arise. Therefore, any suggestions, feedback, or advice on the details of this policy will be highly appreciated and reviewed before being incorporated.

This policy shall apply to all employees.

5 Objectives

All KoTDA ICT facilities and information resources remain the property of KoTDA and not of individuals, teams, or departments. It is in view of this fact that the objectives of this document are thus to:

- enhance compliance with the laws of Kenya
- enhance information security of KoTDA systems.
- enhance best practice as per ISO 27001
- enhance efficient use of information systems by KoTDA employees and the affiliates
- enhance Confidentiality, Integrity and Availability (CIA) of ICT systems
- enhance a spirit of awareness, co-operation, trust, and consideration for others

6 Scope and Legal Regulatory Framework

The ICT policy document relates to all Information Technology equipment and services provided by KoTDA including, but not limited to, email system, databases, ERP, operating systems, internet, telephone systems, wireless communication, printers and copiers. All KoTDA staff, interns, consultants as well as business partners that interact with KoTDA ICT resources are expected to adhere to it.

The KoTDA ICT Policy shall be in compliance with the following Acts of Parliament and Government Policies:

a. The Kenya Information and Communication Act 2013
b. The National ICT Policy Guidelines 2020
c. The Data Protection Act 2018
d. The Computer Misuse and Cyber Crimes Act 2018

6.1 Compliance with the ICT Policy

a. All employees are expected to strictly adhere to the requirements of this policy without exception as they discharge their duties and responsibilities.

b. Failure to follow the Policy and the associated procedures and instructions will lead to disciplinary actions.

c. Any claim of ignorance as to the existence and/or application of this Policy shall not be a ground for justification of non-compliance.

d. Any uncertainty as to the provisions of this Policy or any clarification shall be directed to the Manager ICT and Smart City Solutions.

7 Guiding Principles

This policy shall be guided by the following key principles:

a) Mainstreaming of ICT in the Authority;
b) Seamless integration of ICT;
c) Management of Information Systems (MIS);
d) Alignment and adherence to relevant Acts of Parliament and Government Policies
e) Adherence to the industry's best practices & policies;

8 Policy Implementation

To ensure implementation of ICT the policy, the Authority shall:

a) Assure availability of all anticipated ICT services and systems within the Authority.
b) Assure availability of all anticipated Common Network Services (Network Infrastructure), mainly comprising physical network infrastructure (wiring, switches, routers, servers, etc) and communication protocols (TCP/IP), from the collective/systems, and in conformity with The National ICT Policy guidelines, Data Protection Act, Computer Misuse and Cybersecurity Act, and industry best practices within the Authority.
c) Assure availability and controlled usage of basic user-level data communication and telecommunication services such as e-mail, access to internet/extranet/intranet services and telecommunication terminal equipment.
d) Promote use of the ERP and all its related systems.
e) Promote office computing among staff and partners. Major office computing applications are word processing, e-mail, spreadsheet processing, data and document storage and retrieval desktop publishing, access-to internet, and intranet.
f) Assure availability of core infrastructure and services needed to ensure that Konza can carry out the core functions of a smart city. This collection of infrastructure and services are known as the ***"smart city facilities"***.
g) Continuously improve both the efficiency and effectiveness of investor/customer relationship management through the implementation of an integrated Parcel allocation and customer relationship systems.
~~h)~~ Continuously improve the development of informal/formal linkages amongst partners within the research and innovation space through the implementation of Konza Virtual Innovation Platform.
i) Ensure that all staff are trained on a continuous basis to equip them with the requisite skills to fully exploit the ICT potential in their different functions.
j) Ensure sustainable management of the Authority's ICT resources through the creation of appropriate policy guidelines and regulations, advisory and operational organs that will cater for the broad interests of all users. Such policy guidelines and regulations herein referred to as Appendices will consequently be part and parcel of the ICT policy.
k) Develop and continuously implement the Information Security Management Systems as per ISO 27001.
l) Adhere to industry best practice by implementing COBIT and ITIL framework for all ICT processes and procedures.

m) Provide for the growth of its ICT resources and their financial sustainability through adequate funding and appropriate operational mechanisms.
n) Assure mobility

The CEO shall appoint an ICT Steering Committee as an advisory organ which will constitute the necessary subcommittee and task forces.

9 Policy Statements

9.1 *Copyright*

The Authority may provide proprietary software to staff to facilitate their work activities. Officers are advised to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges. Officers that require specialized software for their day to day work should make requests through their supervisors for the software to be procured based on approved workplan and budget.

9.2 *Security*

9.2.1 KoTDA Systems

The Authority will have in place information systems for enhancement business processes. The ICT division shall be responsible for all information systems in place within the Authority. ICT will grant access to the systems to officers as per their duties and responsibilities. Officers are advised to only access authorized systems. Unauthorized access and manipulation of systems is strictly prohibited and may result in disciplinary action.

9.2.2 Unauthorized Access

It is prohibited to obtain unauthorized access to any systems, computer (including workstations and PCs), servers, network equipment, surveillance equipment and access control devices or to modify its contents. Officers that require access to information resources not accessible to them are advised to contact ICT support.

9.2.3 Confidentiality

Information that is classified as confidential as per the Records Management Policy and ISMS policy must not be copied and or shared without prior authorization of the Authority or the information owner. All confidentiality breaches will be addressed as per the ISMS policy.

9.2.4 Responsibility

Officers are individually responsible for any Authority information in their possession and devices issued to them by the Authority. Officers are advised to lock or log out of their devices when not at their stations. An officer who leaves their PC unattended without locking the active session, will be responsible for any misuse of the device as a result.

9.2.5 Viruses/ Harmful programs/ Anti-Virus

The Authority shall provide anti-virus software for all devices issued to officers, servers and any other computing devices owned by the Authority. The Authority may also issue officers with peripheral storage devices such as external hard drives, flash disks and compact discs.

All peripheral storage devices such as compact discs, flash disks and external drives MUST be scanned for viruses using the installed anti-virus program.

It is every officer's responsibility as a user to read the on-screen anti-virus alerts regarding malicious software, intrusion, updates, and/or any information. Anti-Virus software shall be set to automatically update daily; users are advised not to interfere with the update process on their PCs. Users are advised to contact ICT for help with actions on any alerts.

All servers shall have antivirus software installed on them, officer in charge of systems shall be responsible for this.

9.2.6 Personal/Confidential Information

Officers who in the course of duty record or obtain information about individuals must at all times adhere to the Data Protection Act. Personal or Organization data should be treated with utmost care and confidentiality unless otherwise stated.

9.2.7 Meeting Recordings

The Authority has provided a platform for conducting online meetings, webinars, and live sessions. This platform provides for recording of proceedings. Officers in position to record the proceedings MUST inform the participants of the intention to record the proceedings. The recordings MUST be stored adhering to the highest standards of Confidentiality, Integrity, and Availability.

9.2.8 Electronic Espionage

Any information available within ICT facilities must not be used to monitor the activity of officers in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions to this however are:

i. In the case of a specific allegation of misconduct when the Management Team can authorize accessing of such information when investigating the allegation. This may require denying the officer involved access to ICT facilities pending investigation.
ii. When the ICT Support section cannot avoid accessing such information whilst fixing a problem. The officer concerned will be informed immediately and information will not be disclosed wider than is necessary.
iii. Systems administrators, database administrators and auditors in their day to day work activities.

9.3 Email

Email is considered an official means of communication both internally and outside the Authority.

9.3.1 When to use email

i) Email is preferred to paper for timely communication and reduce paper use.
ii) Use email as a backup to telephone communication and for record and accountability purposes.
iii) The Authority's intranet will be used to communicate all relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information) and notification sent on email.

9.3.2 Use of Distribution Lists:

i) Only send Email to those it is meant for; broadcasts are discouraged unless necessary as they can be disruptive.

ii) Officers who by the nature of their work will be required to broadcast emails are advised to always ensure to blind copy all recipients and to adhere to the Data protection Act and the Computer Misuse and Cybersecurity Act.

9.3.3 General points on email use

i) Officers publishing or transmitting information externally must at all times be aware that they are representing KoTDA and could be seen as communicating on behalf of the Authority.
ii) Officers are advised to keep their email inbox up to date at all times.
iii) Archive old email correspondence that does not require regular reference.
iv) Download attachments only when necessary so as to optimize storage of your PC
v) Officers are advised to be alert to spam emails that may contain phishing and virus attacks. Consult ICT support in case in receipt of suspicious and unsolicited emails.

9.3.4 Email etiquette:

Officers must be aware they are representatives of the Authority at all times when on the Internet using the Authority's corporate email:

i) All emails sent out must not put the Authority in disrepute
ii) Sending or forwarding of obscenities, pornography, drugs or substance abuse, religious extremist information, political propaganda is strictly prohibited
iii) Use relevant subject headers
iv) Use of capital letters in emails is discouraged as it is perceived as shouting.
v) All officers are advised to adhere to the Authority's standard email signature template as per the visual identity document.
vi) Uphold email forwarding etiquette at all times

9.3.5 Delivery & Receipt of emails

For prompt receipt and delivery of emails, officers are advised to ensure:

i) Use of correct email address
ii) The internet connection is up
iii) The internet connection of the recipient is up

Email receipt and delivery may be delayed due to challenges in internet connection and server availability, urgent emails should therefore be followed up with telephone calls. Officers should be alert to failed delivery reports emails and address them accordingly.

9.4 Internet Usage

The Authority will endeavor to provide fast, reliable, and redundant internet connectivity for use by the officers at all times to ensure seamless communication and business operations. Officers will be allowed to use the internet for other uses other than official subject to fair usage and firewall rules put in place.

Access to pornographic, gambling, religious extremism, narcotics, political propaganda and violence websites or content is strictly prohibited and may result in disciplinary action.

9.5 Network Security and Access

The Authority is connected via Local Area Network Internally and Wide Area Network onto the internet. Information and computing resources are offered on these networks through cable and wireless connections.

A Unified Threat Management System shall be used across the entire KoTDA network to monitor and prevent and address all forms of cyberattacks. The officer in charge of systems shall ensure that this policy is adhered to.

All computers connected on the network shall mandatorily have up-to-date antivirus software to prevent viruses and all other forms of attacks. ICT Division shall ensure the UTMS is always updated and licenses are procured in good time.

All officers shall seek authority from ICT before connecting any foreign computer devices to the Authority's network.

9.6 Server Room Access

Only authorized ICT personnel are permitted access to the Server Room. The server room shall have biometric access control installed and a movement control book. All persons other than authorized officers will be required to be registered in the movement control book and accompanied by an authorized officer.

9.7 Printers, Telephones, and Copiers

The Authority provides printers, copiers, scanners, and telephones to facilitate officers in their day to day duties. These resources are available for use by all officers for official purposes and are subject to fair responsible usage.

Officers are discouraged from using these resources for personal purposes. Misuse of the resources may lead to suspension of the officer's user account.

9.8 Passwords

All officers shall be issues with user accounts protected by passwords for all system and resource accounts administered by the Authority. Temporary contractors shall also be issued with temporary accounts with passwords.

i. All systems-level passwords such as network administrator, application administration account users, firewall, website, servers must be changed at least every 45 days.
ii. All account passwords must be changed at least every 90 days
iii. Passwords should be a combination of alphanumeric and special characters (!_?$^*#), i.e. complex, but easy to remember
iv. Passwords must be at least six (6) characters
v. Accounts shall automatically lock after three unsuccessful logon attempts
vi. Password Management
    a. This shall be the responsibility of the officer in charge of systems
    b. A user whose password has expired, or account locked shall (upon request through IT support) be assigned an initial password by the systems officer. The affected user must change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.
    c. Passwords are confidential and must not be shared

d. Passwords must not be inserted into email messages or other forms of electronic communication.

vii. Passwords and their related accounts shall be expired and deleted respectively on:

a. Separation of an officer with the authority, taking into account the separation procedures as per the human resources manuals and policies
b. Expiry of temporary contracts
c. A case of user account being compromised

9.9 ICT Related Training

The Authority shall endeavor to provide capacity building on ICT to ensure its officers are up to date with emerging trends and technologies in the highly dynamic field.

The ICT division shall identify training needs every beginning of financial year and forward to the Management. The Management shall review the training needs as per the HR training policies.

9.10 Online Subscriptions

Some resources used for business operations may require online subscription. Approval for the online subscriptions must be sort from the Chief Executive Officer. ICT will facilitate in consultation with Finance.

Officers are advised against using their personal cards for online subscriptions. The Authority shall not be liable for any losses incurred through unauthorized online transactions.

9.11 ICT Disaster Recovery

The Authority shall have a disaster recovery and business continuity plan. All ICT disaster recovery shall be carried out in line with the approved Authority's business continuity and disaster recovery plan.

The CEO shall appoint a disaster recovery team with representation from all key divisions who will be responsible for:

- implementing the disaster recovery plan.
- ensuring minimal disruption of business operations, assuring a reliable and sound backup system, minimizing risks of delays, ensuring the maximum security level and aid whenever needed in speedy restoration of operations and any other actions which are part of the disaster recovery plan.
- analysis of existing network or IT structure, applications, databases, and organizational setup
- maintaining a master list of all storage locations, inventory, customers, forms, policies, and alternate locations for operations.

9.12 ICT Helpdesk

The ICT division shall establish and run an ICT helpdesk solution. All ICT technical assistance requests shall be channeled through email and/or telephone to the relevant ICT helpdesk. The helpdesk shall prioritize the requests based on severity and chronology or reporting. The helpdesk shall be guided by the ICT divisional internal service level agreement.

9.13 Change Request

The Authority runs various systems bought off the shelf and customized. Over time new requirements in functionality and process may arise that will require changes to the existing systems.

All systems change requests will follow the laid-out change request procedure. The requests will have to be generated by the user, forwarded by the Head of Department, and approved by Head of ICT. The approval will be dependent on available budget and the contract terms of the service provider.

The changes will only be made once approval is done and budget is availed. The change process will take into consideration minimum disruption of business processes and loss to the Authority. The changes will be implemented at low peak hours to ensure minimal interruption.

9.14 Computing Devices Issued by the Authority

The Authority shall issue all officers with computing tools, devices and accessories to aid in their delivery of duties. Such devices may include computers, tablets, telephones, printers, scanners, external hard drives, flash disks, cameras, voice recorders. All items issues by the Authority shall remain the Authority's property. Capital asset items shall be tagged in consultation with the Procurement department. The officer shall bear full responsibility over any device issued by the Authority and shall exercise duty of care.

In case of loss or damage, the officer responsible shall file a report to the head of Human Resource and Administration with a copy to ICT. The report shall include full details on the circumstances of loss/damage and data contained in the lost or damaged devices.

ICT in consultation with Human Resource and Administration will review the circumstances and agree on terms of replacement of the device.

9.15 Maintenance of ICT equipment

The ICT division shall be responsible for maintenance of all ICT related devices and equipment. ICT shall ensure availability of basic service and repair tools and resources to attend to minor equipment service and repairs.

In consultation with Procurement, ICT shall engage service providers to carry out regular maintenance of ICT equipment and devices to ensure optimal operating condition at all times.

9.16 Replacement of ICT Equipment

ICT equipment is subject to age and obsolescence. The ICT division will therefore in consultation with Finance and Procurement actively budget for upgrades of existing and devices every financial year or as per requirements. It is the responsibility of officers to report aging and or broken-down equipment and devices to allow for prompt replacement.

9.17 Business-Critical Third-Party Software

The Authority shall endeavor to provide all the required software tools to officers to facilitate their day to day work. However, it is the responsibility of the officers to make official requests for approval through their Heads of divisions or departments. ICT shall facilitate with developing the best specifications and in consultation with Procurement and the officer procure the correct software for use.

Officers are advised to make the requests in good time to allow for timely budgeting and inclusion in the annual workplan.

9.18 Care of equipment:

An Officer shall be personally responsible for all ICT equipment issued to them. Officers are therefore advised to ensure security and care of the equipment issued by the Authority to ensure they always remain safe and in good working condition.

Officers are advised against taking food or drinks when handling any ICT equipment.

10 Effective Date

This policy shall come into effect on XXXXXX

11 Policy Review

This policy will be reviewed every three years or as and when need arises.

12 Other Particulars of the ICT Policy

Implementing Unit	Xxxxx Department
Effective Date	
Review Date	
Policy Version/ Revision History	DRAFT 0
Scope of Policy Application	All KoTDA Stakeholders
Approval by the CEO:	
Approval by the Board of Directors:	