IPOA Independent Policing Oversight Authority

INDEPENDENT POLICING OVERSIGHT AUTHORITY

1st Ngong Avenue, ACK Garden Annex, 2nd & 3rd floor | P. O. Box 23035 00100 Nairobi, Kenya
Tel: +254 725 327 289 / 732 081 490 / 734 504 790 | E: info@ipoa.go.ke, W: http://www.ipoa.go.ke

Information Communication Technology (ICT) Policy

MAY 2015

Preface

Information and Communication Technology (ICT) is a crucial enabler in the achievement of IPOA's Mandate. It is in recognition of this that, IPOA has formulated this policy to provide guidelines on how ICT services and infrastructure will be availed in the Authority and provide a framework for the planning, implementation and usage of ICT resources in the Authority.

In order to execute its mandate, the Authority uses ICT services for enhanced efficiency. In provision of such services, the Authority commits to ensure that adequate resources are provided to implement a reliable and appropriate IT infrastructure. It is imperative thus that acquisition and usage of such facilities requires to be governed by an organization wide ICT policy.

This policy document provides a framework for ICT Service delivery, governance and resources in the Authority in conformity with the existing government policies, legal and regulatory framework.

Acronyms

CD – Compact Disk

ICT Dept – Information Communication Technology Department

DRS –Disaster Recovery Site

DVD – Digital Video Disk

ICT – Information and Communication Technology

ISO – International Organization of Standards

IT – Information Technology

IPOA – Independent Policing oversight Oversight Authority

LAN – Local Area Network

NPSC – National Police Service Commission

KPS – Kenya Police Service

PABX – Private Automatic Branch Exchange

PC – Personal Computers

SAN –Storage Area Network

SLA – Service Level Agreement

WAN – Wide Area Network

Table of Contents

1.0 Introduction

The Independent Policing Oversight Authority, herein referred to as IPOA or Authority, was established through an Act of Parliament No. 35 November of 2011 to provide for civilian oversight over the work of the police in Kenya. In order to execute its mandate, the Authority uses ICT services for enhanced efficiency. In provision of such services, the Authority commits to ensure that adequate resources are provided to implement a reliable and appropriate IT infrastructure. It is imperative thus that acquisition and usage of such facilities requires to be governed by an organization wide ICT policy.

To address this need, the Authority has developed this ICT policy in line with the existing government policies, legal and regulatory framework.

2.0 Objectives

This policy seeks to;

a. Ensure provision of adequate and reliable information systems in the Authority
b. provide guidelines on the usage of ICT software, hardware and services in the Authority
c. ensure information security of Authority systems and data
d. Promote efficient utilization of information systems within the Authority employees and any other partner agency as may be approved by the board from time to time.
e. ensure application of best practices and standards
f. Promote spirit of awareness, co-operation, trust and consideration for others.

g. Training of All IPOA Staff on ICT hardware and software equipment.

3.0 Scope

This ICT policy covers all IT facilities, hardware, software, and services provided by the Authority. These are:

a) Facilities

i. Data generation/processing centre within the authority
ii. Meeting/Training room within the authority
iii. Server room(s)
iv. ICT maintenance room
v. Data Recovery Site(s) (DRS)
vi. All ICT facilities installed or to be installed in areas upon devolution of IPOA services to counties.

b) Services

i. Provision of guidance and expertise training in ICT

ii. ICT support in software, hardware and any other computing infrastructure
iii. Technical support to all IPOA personel

c) Hardware

i. PCs
ii. Laptops
iii. Printers
iv. Scanners
v. Servers
vi. Network routers, firewall and switches
vii. Power backup equipment (e.g. Uninterruptable Power Backup - UPS)
viii. L.C.D Projectors
ix. Network Devices
x. Cameras (Digital and Camcorders)
xi. IPADs, tablets, Smartphones and other Mobile Computing Devices
xii. Diskettes/CDs/DVDs
xiii. Flash-disks/external hard-disks
xiv. PABXs, Telephone heads, fax and photocopiers
xv. All other ICT related hardware

d) Software

i. Network operating systems
ii. PC operating systems
iii. Application software
iv. Utility software
v. Custom made systems
vi. All other ICT related software

e) County Offices

The policy will cover all county offices and branches to be created in future after devolution of IPOA services to counties. These areas will be supported from the Authority headquarters.

f) Gender

The policy caters for persons of all genders without discrimination in line with the national policy on gender.

g) Disability

The policy caters for persons with disabilities in that the Authority will endeavor to provide specialized equipment and services to disabled persons so as to enable them make maximum use of ICT services.

4.0 ICT Facilities Usage

a. All ICT facilities owned by the Authority will be issued to its staff for official use through the ICT Department. The Department will be the custodian of ICT systems including software, and hardware as a measure to facilitate standardization. Thus officers will be availed hardware, software and systems relevant to their work requirements. All portable ICT equipment including laptops, projectors will centrally be controlled by the ICT department and issued as required by the users who will be responsible for returning them after use. A register for such portable ICT equipment shall be kept and updated on loaning and returning of the items.
b. Staff shall take maximum care of such facilities and ensure responsible and secure usage.

c. Users shall not relocate, repair, reconfigure, modify IPOA ICT equipment or attach external devices other than for data storage to such equipment without the authority from ICT with the exception of ICT workstations or laptops being used outside the institution after being registered with the ICT department.
d. Staff may use external disks only for the purpose of storing official information. Such external disks must be scanned for viruses and other harmful software.
e. Personal software, hardware or systems shall not be used within IPOA LAN. Staff should notify the ICT department when using any of these personal software hardware or systems
f. Precaution should be taken when having food or drinks close to any ICT equipment.
g. IPOA ICT team shall deactivate access credentials once one ceases to be an employee.

5.0 ICT Security

a. All IPOA systems and information shall be effectively protected against unauthorized access through user rights roles and access levels.
b. The ICT Department shall provide network service to staff to transmit data to requesters and store data files in an authenticated central server.
c. Users within same Department/working group will be given access level that allows them admission to their files/folders.
d. For traceability and identification, all hardware shall be bar-coded and included in the IPOA asset register. This shall include any

hardware bought for /donated to IPOA.

e. ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided through user passwords based on roles and access levels and physical security inform of lockable cabinets or drawers.
f. Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.
g. Portable computing equipment issued for short term use shall be stored in secure lockable cabinets.
h. An updated register of all ICT equipment e.g. LCD projectors issued out to authorized personnel shall be maintained.
i. All data storage media shall be stored in secure environments that meet manufacturer's specifications for temperature and humidity.
j. Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.
k. Any non LAN-connected and official computing equipment should be subjected to period antivirus updates as advised by ICT from time to time.
l. Any use of ICT software and hardware by any staff or authorized person shall be allowed only after receiving authority from CEO on their terms of engagement.
l. All ICT hardware or software will not be taken off-site from IPOA offices, for servicing and /or upgrading without written authority from ICT.

6.0 The Internet

a. All connections to the Internet within IPOA offices shall be implemented through the IPOA Internet connections via a

firewall/proxy.

b. To protect IPOA systems from Internet attacks or denial of service by Internet malware, all software downloads shall be authorized by ICT. Such a download will be passed on to the requester only if it passes the ICT security tests and if it is permitted for free use by its manufacturers.
c. No copyright material shall be downloaded from the internet or utilized in breach of its license agreement.
d. Internet services shall be provided only through the IPOA Internet connection or IPOA USB modems or any other approved gadgets.
e. To optimize internet bandwidth usage, Authority's network shall not be used to stream music, unauthorized websites and video as these lead to deprivation of the same capacity to legitimate users during normal working hours except, where such permission is granted by ICT in writing.
f. IPOA internet and network resources shall not be used to access or transfer any material containing:
    i. Derogatory remarks based on race, religion, gender, physical disability.
    ii. Images or references that may be considered to be offensive or in breach of any law or regulation.

7.0 Network Access & Permissions

a. Each user will have only one personal identification code (User ID/user name and password) with necessary access levels and privileges.
b. Users will be given initial default password which they will be required to change on first logon to the system.
c. A user whose password has expired, or account locked shall (upon

request through IT support) be assigned an initial password by the systems administrator. 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.

d. User IDs will be consistent in structure i.e. the first letter of the first name and last name, all in lower cases (ignoring middle names). If this combination conflicts with another user, then the first letter of second name will be used as the second letter of the user ID. If the officer does not have other names, then letter 'a' through 'z' will be used so that user ID is unique within IPOA access systems.
e. All devices will require access credentials (user ID and password) to be accessed over the network. Guidelines on structure of user IDs and passwords will be provided by ICT Department.
f. Users will be responsible for the confidentiality of their access credentials and prevention of any unauthorized access to ICT equipment. Any attempt to use other users' credentials to gain access to network resources is strictly disallowed. Any account found to be compromised or shared shall be discontinued and a new one issued where necessary.
g. Only authorized personnel are allowed access to ICT resources
h. Access credentials shall immediately be deactivated and confirmed in a clearance certificate by the ICT once a member of staff ceases to be an employee of the Authority.
g. ICT is authorized to gain access to a user account and folders if that account is suspected to have breached systems security or is in violation of this policy.
h. The ICT Department shall enforce standardization of systems and network configuration, including directory structures, to simplify network management.

8.0 Website

a. The ICT department shall ensure that the IPOA Website upon authorization by the Communications and Outreach department is kept in an updated status at all times. By use of the latest technology, the website shall be maintained in a user friendly and accessible state.
b. All requests for changes on the website shall be subject to the approval of the CEO.
c. The ICT Department shall ensure that the website is always available to the public.

9.0 ICT Equipment Maintenance.

a. The ICT shall ensure that all ICT equipment is kept in proper working condition at all times.
b. All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.
c. Quarterly maintenance of ICT equipment shall be carried out by the ICT team following laid down maintenance procedures and standards to ensure proper working condition.
d. In areas where the Authority lacks adequate internal capacity, annual maintenance contracts will be entered into with service providers.

10.0 Email Usage

a. Staff shall be issued with official standardized e-mail addresses as outlined in the section above.
b. All official email communications shall be through official email

addresses. ICT will ensure that mail service is available to staff always.

c. The IPOA Intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).
d. Email users shall avoid broadcast communication (i.e. sending to large groups of people using email aliases) unless where absolutely necessary. One must always ensure proper audience segregation is used before sending an email.

e. Group email shall be allocated on request by heads of departments. The ICT Department shall create group emailing rules to ensure mail circulated within the group can only be done by approved email account and promote mail etiquette.

f. IPOA mail service shall not be used to broadcast other unofficial information or requests (e.g. information or opinions on political matters, social matters, and personal requests for information etc.)
g. Emails with attachments greater than 15MB will require authorization from ICT. This will remove unnecessary load on the network and the mail server so as to guarantee equitable bandwidth sharing by all staff.
h. It is due to this complexity that, urgent mails should be given at least 15 minutes for delivery and followed up through telephone. Users receiving NDR (Non-Delivery Reports) for mail failures shall forward the same to ICT Support or ICT Systems Administrators for trouble shooting. Staff are however required to ascertain, before launching a complaint that the address of the recipient is correct and free from typos.
i. Complaints about mail receipt failure should always be accompanied by the sender address and the recipient address. This will enable the

administrators to narrow down to the particular case and give a report and advice to the affected user the soonest possible (within 30 minutes or as per the SLA).

11.0 Internal ICT Support

a. Logging incidents and service requests; all ICT related incidents and service requests, without exception, must be reported to the service desk in the first instance. Users must not call individual ICT officers or third party service providers directly.
b. Users may use either telephone or portal to log incidents and service requests.
c. The following information should be provided; contact details-Name, department, telephone number and location; Nature of incident or service request any error message; Equipment reference number.
d. Where appropriate, the IPOA ICT service desk coordinator will discuss the priority to be assigned to an incident based on prioritization guideline.
e. Service requests will be allocated a target achievement date. This may be revised subsequently by ICT staff dealing with the ICT incident/request. It is responsibility of the ICT staff to keep users informed of changes to the target date.
f. The user is notified of the ICT service desk reference number either at the time of reporting by telephone or from the display on the portal.
g. Service desk response; the ICT team will deal with request as soon as possible, dependent upon the priority allocated. Target times are contained in Appendix I.
h. ICT staff will provide regular updates to the user during the resolution period. In the event of a query, the ICT service desk should be first

point of contact. Users of the portal can view updates on their open ICT incidents/service request at any time.

i. ICT incidents/service request will not normally be closed until the user has confirmed a satisfactory resolution. If attempts to contact the user are unsuccessful then the incident/service request will be closed and recorded as resolved after a period of one week.

j. Users Responsibility; IPOA ICT officers will make visits to sectional offices where necessary and will inform the user in advance. Users are responsible for ensuring that ICT staff have access to the relevant IPOA ICT equipment and applications. Users are also responsible for ensuring that staff seeking are carrying valid Trust identification.

k. Exceptions; The ICT Department does not provide support for:- Equipment or software purchased/ installed without agreed trust policy and procedures.

l. Response times do not apply where ICT incidents/service requests arise as a result of unauthorized interventions.

m. While IPOA will strive to provide ICT support services, officers assigned to hardware must ensure they are not exposed to risks that can cause their damage.

n. ICT officers will be available to offer technical support on any software or hardware upon users' requests.

o. Where applicable, equipment to be used out of office shall be accompanied by an ICT Technician to ensure proper packaging, offloading and installation at destination.

p. Escalation procedures; If a user requires an ICT incident/service request to be escalated they should contact the ICT service desk with the ICT incident/service request reference number and ask to speak with the ICT administrators or alternatively email ictservice@ipoa.go.ke.

12.0 Out-Sourced ICT services

a. The Authority shall out-source ICT equipment and/or services whenever such capacity lacks in the Authority with approval from the Director, Business services upon recommendation from ICT. Such a need shall be supported by a needs assessment report from ICT.
b. Acquisition of such services will be guided by the Public Procurement and Disposal Act (PPDA), 2005, IPOA procurement procedures and Public Procurement and Disposal Regulations (PPDR), 2006 or any law amending or replacing the same.
c. All out-sourced ICT equipment and services will be supervised by ICT in accordance with Service Level Agreements (SLAs) that are signed in consultation with ICT.
d. The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the ICT Department.

13.0 Acquisition and Disposal of ICT Facilities

a) Acquisition of ICT Facilities

i. Acquisition of ICT facilities shall be guided by the Public Procurement Procedures and Guidelines in the Public Procurement and Disposal Act (PPDA), 2005, Public Procurement and Disposal Regulations(PPDR)2006, Best Practices and the IPOA Procurement Manual. Where funds are donated from external sources, the respective donor conditionalities, terms, agreements or memoranda of understanding shall apply.
ii. All User requests for acquisition of items of ICT nature shall be

channeled through ICT who will confirm lack or availability of such items in the Authority. If not available, ICT will prepare specifications in consultation with the requesting Department and forward the request to the Director, Business services for approval.

iii. In order to minimize the costs, IPOA will standardize software and hardware to be used within the Authority with advice from ICT. This will be reviewed annually as need arises.

iv. All Departments' will forward to ICT their software and /or systems needs who will offer technical guidance and support in facilitating the acquisition process.

v. ICT goods, related services and/or works once acquired will be received by the Authority's Procurement department and inspected by Inspection and Acceptance Committee in line with The Public Procurement and Disposal Act (PPDA), 2005 and Public Procurement and Disposal Regulations (PPDR), 2006 framework. The Committee shall seek professional assistance from ICT.

vi. The ICT Department shall ensure that all software licenses in use in the Authority are promptly renewed to guarantee smooth Authority operations and continuous software updates and support from manufacturers.

vii. The Authority will strive to maintain reliable hardware infrastructure by upgrading aging ICT equipment every three years.

viii. In order to avail adequate and reliable computing capacity to the technical staff, the Authority shall provide at least one functional computer to every technical staff both at the headquarters and at the future county branches to be established once services are devolved to counties.

b) Disposal

i. ICT shall identify hardware and software to be disposed and liaise

with Procurement Department for assessment leading to disposal as per PPDA, 2005 and the PPDR, 2006.

ii. ICT shall ensure that all equipment earmarked for disposal are cleared of Authority data and storage media destroyed.

iii. Upon receiving requests for disposal ICT Services will:

- Check the IT equipment inventory to establish if any other part of the authority has older equipment which can be exchanged (taking into account IPOA priorities) and if so, consult with the appropriate service provider and make an exchange.
- Remove any useful parts for spares.
- Re-harvest any unused software license.
- Dispose of equipment ensuring that regulatory and legislative requirements are met including effective data destruction of all stored information, particularly pertaining to sensitive data i.e. personal or cardholder data, to a state that it cannot be recovered.
- Some components, such as TFT monitors will always have a value to the organization as long as they are operational – ICT Services will arrange exchanges for bigger monitors that become available.
- In the case of IPADS, Tablets and Mobile Telephones, based on the net book value depreciating formula that will be provided by Finance department, the value of the item will be determined and a member of staff leaving IPOA will pay this amount to own the item. All ICT items given to users for use in their daily operations should be surrendered to the ICT department for clearance.

14.0 Backup & Disaster Recovery

a. IPOA' information resources such as data, business contacts, emails, text documents, presentations, contracts, accounts and other valuable information shall be safely preserved in a recoverable state.
b. ICT Department will maintain consistent automated backup mechanisms to preserve IPOA data in a distributed Storage Area Network (SAN) and at a DRS in order to ensure data recovery in the event of accidental loss.
c. All IPOA data shall be saved in organized shared folders in allocated branch servers from where they will be backed up in SAN and Disaster Recovery Site (DRS) through synchronized mechanisms in addition to tapes or external drives in accordance with the IPOA Back-up Plan.
d. Network and server administrators will ensure that data is copied to these allocated servers and in all other backup destinations.
e. It is the responsibility of the respective users of any non LAN-connected computing equipment (including laptops/notebooks) to arrange with the server administrator for the transfer of official data from these non LAN-connected equipment to the relevant server folders every day or whenever practical.
f. Any unofficial files shall not be allowed on IPOA Servers.
g. Only authorized personnel will be able to visit off-site DRS.
h. To implement an ICT seamless backup service, all officers connected to IPOA LAN shall login to centralized authentication servers. Officers working from remote locations will be required to dock to the IPOA network to back up official data.

15.0 Printers, Telephone Lines, Fax, Scanners and Copiers

a. IPOA Staff are expected to use the above peripheral devices responsibly. Irresponsible or usage of these facilities for personal gain is prohibited, and may lead to denial of the service and/or surcharge.
b. Where possible, users are required to print on both sides of the paper. ICT support team will give guidance on how various printers are able to print on both sides.
c. Printers will be configured to be shared by many users and placed in secured open offices where possible.
d. An electronic document scanner shall be used to minimize usage of fax machines, printers and copiers, saved in suitable formats and emailed to recipients.

16.0 ICT Training

a. Authority's ICT training needs shall be assessed by the ICT Department and recommendations captured in the Authority's training plan.
b. The ICT shall recommend ICT trainings relevant for every section and forward requirements to HR and Director, Business services.
c. IPOA staff will be trained on emerging technologies as the Authority may determine from time to time in consultation with ICT.

17.0 Online Subscriptions for IPOA products

a. Directorate/Departmental shall have the mandate to do online subscriptions on behalf of their directorates/departments, but in consultation with the Head of ICT department. For security reasons, the directorates/departments heads shall use a credit card provided by the Authority. Presentation of proof of payment should be provide. All procurements should follow the procurement regulations of the Authority

18.0 Enforcement and Control

a. Deliberate breach of this policy statement may lead to disciplinary measures in accordance with IPOA Human Resource Manual. These may include but not limited to the offender being denied access to computing facilities or surcharge for the loss or abuse of ICT facility or service.
b. Whenever surcharge is imposed on negligence as noted in (a) above, due process will be followed in imposing the surcharge.
c. Unauthorized access to information, facility or computer (including workstations and PCs), over the network or to modify its contents is strictly forbidden.
d. Officers within IPOA network shall not write, publish, browse, bookmark, access or download obscene, pornographic or pedophilic materials.
e. All hardware, software and /or systems in use in IPOA stations shall be licensed. Any officer using unlicensed products shall bear legal consequences for the product as per 'the Copyright Act, 2001'

19.0 Privacy and Confidentiality

a. The Authority shall guarantee right to privacy and confidentiality of individual staff information while discharging ICT services.
b. Information/services/resources available within IT facilities will not be used to monitor the activity of individual staff in any way (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. Without limitation to this provision, the following shall be excluded:
    i. In the case of a specific allegation of misconduct or for any

other investigation purpose, the Director, Investigation may authorize access to such information or denial of service while the staff is under investigation.

ii. Where the ICT Department or any other Authority directorate/department cannot avoid accessing such information whilst administering, resolving ICT systems problems or in their day to day work activities.

20.0 Revision

This policy shall be revised every three years or as and when need arises under the authority of the Director, Business Service or the ICT board committee, to keep in tandem with changes in technology, statutory regulations or for any other purposes as may be advised from time to time by ICT.

References:

i. National Policy on Information and Communication Technology (ICT); GoK, 2012.

ii. ICT Standards and Guidelines. Department Of E-Government. Kenya (2012)

iii. ICT Policy Formulation and E-Strategy Development. A Comprehensive Guidebook. Asia-Pacific Development information Programme, UNDP, 2012.

Public dispoal act and any other.

APPENDIX I

The ICT Department aspires to achieve the response times below. However, users must be aware that the resolution of some ICT incidents/service requests will be outside of the Trust's i.e user rights and access levels control and may be subject to other service level agreements. In addition, further prioritization may be necessary in busy periods.

Response Times

Priority	Target Response Time	Target Resolution Time
Critical	1 hour	2 hours
High	4 hours	8 hours
Medium	1 day*	1 week
low	2 days*	4 weeks

*Working days: - weekdays excluding public Holidays

Response Time: is the time taken from an ICT incident/service request being logged with the ICT Service Desk to a response being received by the requestor from an ICT Support Technician concerning the nature of the problem.

Resolution Time is the time taken from an ICT incident/service request being logged with the ICT Service Desk to the problem being resolved to the satisfaction of the customer.

BOARD APPROVAL

These ICT Committee Terms of Reference were approved by the Board on ...../...../2015.

Signed: .....

IPOA C.E.O

Signed: .....

Chair, ICT Committee

Signed: .....

Chair, IPOA Board