# GOVERNMENT OF MAKUENI COUNTY

## ICT ADMINISTRATIVE POLICY

# GOVERNMENT OF MAKUENI COUNTY


# INFORMATION COMMUNICATION TECHNOLOGY ADMINISTRATIVE POLICY

## DEPARTMENT OF EDUCATION SPORTS & ICT

**2020**

## FOREWORD

The Government of Makueni County recognizes ICT as a key enabler in its contribution to socio-economic development, and as a vital pre-condition for success of other sectors as envisaged under the Makueni County CIDP 2018 – 2022. Further, Makueni County Vision 2025 points at improving ICT to facilitate development with the view of providing opportunities both to the public sector by ensuring cost effectiveness and efficiency in service delivery and the private sector by providing favorable environment and opportunities to advance technology. The Kenya Vision 2030 anchors the use of Science, Technology and Innovation (STI) in a modern economy with the role of wealth creation, social welfare and international competitiveness, while at the same time adopting a knowledge-based economy being a critical factor for rapid growth.

The administrative policy is an outcome of a broad-based comprehensive and consultative coverage of the evolution of ICT. The initiative to formulate and implement an ICT policy in Makueni is inspired by the need to align the county with national ICT regulatory frameworks, demystify and adapt to the ever-changing global technological environment and align the county to the three underlying pillars (Economic, Social and Political) of Vision 2030. The county of Makueni seeks to thank all the stakeholders for their concerted and supportive efforts, both local and national for the successful formulation and also towards the implementation of this Administrative policy.

In conclusion, it is my conviction that this Policy will continue to set the pace and give the right direction on management of the ICTs within the County Government.

**Dr. Naomi Makau**

**County Executive Committee Member - Education, Sports & ICT, Makueni County**

## ACKNOWLEDGEMENT

The development of this policy document has taken close to four years with involvement of a wide array of stakeholders and actors. The Department appreciates the efforts, commitment and synergy including time invested by all parties who participated in the formulation, development and finalization of this policy. Very special gratitude goes to the Technical Committee led by Dr. Naomi Makau (CECM – Education, Sports & ICT) and members drawn from the Department of Education, Sports and ICT; Legal; Monitoring and Evaluation; and Office of the County Secretary.

The Team effort and tenacity in development of this policy is highly appreciated. We do take cognizant of all stakeholders who critically supported technically in the shaping and compilation of this policy. Further, the Department is indebted in the participation of key informants and partners for their insights during the need's assessment exercise. We thank Cecilia Mutua, (Director ICT), and officers in the ICT directorate, for their commitment in the development of this policy.

Most of all we thank His Excellency Governor Prof. Kivutha Kibwana and Her Excellency Deputy Governor Adelina Mwau whose profound leadership and guidance provided the department with immense wealth of knowledge in formulating this policy. It is not possible to thank everyone by name who contributed towards the development of this policy. Kindly accept our deepest appreciation.

**Rael Muthoka**

**Chief Officer – Sports and ICT, Makueni County**

## Table of Contents

## PREAMBLE

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. GoMC is not an exception. The County Government recognizes the importance of ICT. It is, however, faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance. This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by both GoMC employees and business partners.

## ACRONYMS

**ICT**- Information & Communication Technology

**GoMC**- Government of Makueni County

**RFC**-Request for Change

**RFQ**-Request for Quotation

**RFP**-Request for Proposal

**PT**-Project Team

**BCP**-Business Continuity Plan

**DRP**-Disaster Recovery Plan

**PC**-Personal Computer

**ID Card**-Identification Card

## 1.0 INTRODUTION

### 1.1 Purpose

Information exists in many forms; printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversations; and is the most valuable asset of the county government. The goal of this policy is to provide guidelines for compliance, acceptable and secure use of information communication technology by both GoMC employees and business partners.

The GoMC is committed to improve the livelihood of its citizens by ensuring the availability of accessible, efficient, reliable and affordable ICT services. This is by preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the county in order to preserve GoMC's public image, service delivery, legal, regulatory and contractual compliance.

### 1.2 Scope

The ICT policy document relates to all Information Technology facilities and services provided by GoMC including, but not limited to, email system, databases, applications (software), computers, internet, telephone systems, wired and wireless communication, radio communication, printers and copiers. All GoMC employees, guests, volunteers, and other stakeholders are expected to adhere to it. The document shall be effective from the date of approval.

### 1.3 Responsibility for Implementation

The Accounting Officer in charge of ICT shall have the responsibility and authority to cause this ICT policy to be implemented and maintained. The policy shall be created and/or updated by ICT, reviewed and recommended by the cabinet, and approved by the Governor. The ICT policy shall be issued on a version controlled basis by the Accounting Officer.

*It shall be the responsibility of ALL GoMC staff members:*

#### 1.3.1 Security

- To safeguard their data, personal information, passwords and confidential data.
- To choose their passwords wisely and to change them periodically.

- To follow the security policies and procedures established to control access to administrative data.

### 1.3.2 Respect for Copyright laws & Licensed Programs/Data

To respect the legal protection provided by copyright and licensing of programs and data, for example, not to make copies of a licensed computer program to avoid paying additional license fees.

### 1.3.3 To respect the intended use of Systems for Electronic Exchange

To respect the intended usage of systems for electronic exchange (such as World Wide Web, email, etc.); for example, not to send forged electronic mail, that will intimidate or harass other users, chain messages that can interfere with the efficiency of the systems, or promotional mail for profit-making purposes.

Not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.

### 1.3.4 To report any violation of the IT Policy

To report any information concerning instances in which the County Government's ICT Policy or any of its standards and codes of practice has been or is being violated.

*It shall be the responsibility of ALL senior staff to:*

Implement this policy within their business areas, and make sure it is adhered to by their members of staff;

Make sure that all staff within their business areas undergo appropriate awareness training in support of the goals of this policy.

### 1.4 Enforcement/Compliance

Each staff member of GoMC or Contracted staff shall be required to individually commit that he/she has read and understood this policy and that he/she agrees to uphold such values and policy statements and abide by them at all times. Any staff member found to have violated this policy or any of the supporting policies may be subject to remedial action by ICT Directorate and/or disciplinary action in accordance with the Human Resources Disciplinary Policy.

### 1.5 Change/Version Control

This ICT policy shall be Version 1.1.0.

**1.6 Approval by the Executive Cabinet**

**SUBMISSION:**

Submitted to the County Executive Committee by CECM Education, Sports & ICT:

Name; Dr. Naomi Makau

Signature;

Date; 17. 11. 2020

**APPROVAL:**

This Education & Training Policy is hereby approved by the County Executive Committee during the.....133RD..... meeting held on....17.11.2020

Governor/Deputy Governor;

Name; KIVUTHA KIBWANA

Signed;

Date; 17/11/2020

## 2.0 ICT POLICY ORGANIZATION

### 2.1. ICT Policy

#### 2.1.1 Purpose & Scope

This section emphasizes the need for Cabinet ratification and management support for the policy. It also acknowledges that this policy is a live document subject to annual review in case new changes occur in ICT.

#### 2.1.2 ICT Policy Approval

GoMC shall put in place a suitable ICT policy and obtain Cabinet approval. This policy shall be distributed and communicated to all employees together with supportive guidance and compliance requirements.

#### 2.1.3 Senior Management Support

Senior management is required to actively support, and take responsibility for the implementation and maintenance of ICTs in their respective capacities in a positive and pro-active manner.

### 2.2 ICT Organization

#### 2.2.1 Independent Review of the ICT Policy

An independent review shall be carried annually on the GOMC's overall ICT processes to ensure they are adequate, complete, fit-for-purpose and enforced. The ICT policy shall be reviewed and evaluated annually and also if changes occur in the organization that affect a particular approved policy statement.

#### 2.2.2 Sharing Information with other Organizations

Information regarding ICT issues shall be shared with other organizations in order that risks and vulnerabilities may be better understood and safeguarded.

## 3.0 EMAIL POLICY

### 3.1 Purpose and Scope

### 3.1.1 Definition

E-mail access is provided to staff for the purpose of increasing overall productivity within GoMC and therefore should be used primarily for business activity. The purpose of this policy is to ensure that all staff use email services in a proper and lawful manner.

This policy applies to all staff and other authorized persons with access to GoMC's email services.

### 3.1.2 The Policy

- All communications requiring the use of emails MUST be done through the use of the official emails. Personal emails shall not be used to transact any County Government business.
- All email accounts assigned to staff and other authorized persons shall remain the sole property of GoMC.
- All staff members are responsible for conducting themselves in an ethical and lawful manner when using email.
- Email communication may be monitored under special circumstance with proper authorization from management, for instance, when investigating or monitoring abuse of ICT resources.
- When creating email messages, staff are expected to follow similar standards required in a written business communication.
- All email accounts shall be allocated an equitable storage space. Upon exceeding the allocated storage quota, e-mail messages shall be archived to save server space.
- Email size may be limited depending on bandwidth availability and server performance. Sending email messages to 'All Users' shall require authorization.
- When using email services, staff shall be required to abide by the country's laws, rules and regulations. The GoMC will have standard email addresses for all employees which will be in a format firstname.secondname@makueni.go.ke, designation@makueni.go.ke or group@ makueni.go.ke.
- To enhance institutional memory, officers with multiple accounts should use designation@makueni.go.ke for all correspondence.

- The policy governing passwords will also apply to all email passwords.

### 3.1.3 Email Security

The encryption of email is not necessary in most situation. However, confidential messages shall be secured using the appropriate technology. All staff can access the email accounts outside the GoMC. To safeguard GoMC's data, observe the following:

- Don't print to a public printer.
- Make sure no one is overlooking your screen as you access the data.
- Don't save to a public computer.
- Passwords are the best defense against unauthorized use of a staff's email account. Staff member shall therefore observe the password guidelines to ensure optimum security of their password.
- Email accounts not used for 90 days will be deactivated and possibly deleted.

### 3.1.4. Guideline for Effective Use of Email

Use the email tracking facility to determine if an email has been delivered and opened. This is important when emails require urgent attention. Since work and other services request may be sent by email, it is every staff member's responsibility to check their mail boxes.

As a matter of practice, official email should be copied to superiors and/or relevant staff for information. Care should be taken when addressing messages. The messages should be appropriately addressed so that they can reach their intended recipient(s), spelling and other grammar checking before the message is sent.

### 3.1.5 Prohibited Use of Email

Although by its nature, email seems to be less formal than other written communication, the same laws apply.

It is strictly prohibited to: -

- Send or forward email containing defamation, offensive, racist, discriminatory on the basis of the race, gender, nationality or ethnic origin, age, marital status, sexual orientation, religion or disability.
- Send mail that contains a threatening/violent message or any that is suspicious. If you receive an email of this nature, you must promptly notify ICT directorate.

- Send unsolicited email message, spam, chain letters or advertising.
- Forge or attempt to forge email messages.
- Send email messages using another person's email account.
- Copy a message or attachment belonging to another user without permission of the originator
- Disguise or attempt to disguise your identity when sending email
- Exchange proprietary information, GoMC secrets, or other confidential information with anyone not affiliated to the GoMC.
- Send email that contains violated material protected under copyright laws.
- Distribute GoMC's information to people outside the GoMC without proper authorization.

### 3.1.6 Sending Electronic mail (E-mail)

Email shall only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an email shall only be permitted after confirming the classification of the information being send and then having scanned and verify the file for the possibility of virus or other malicious code.

### 3.1.7 Receiving Electronic mail (E-mail)

Incoming email shall be treated with uttermost care due to its inherent information security risk. Unsolicited or suspicious e-mails should be treated with care until the sender has been identified. The opening of email with the file attachment is not permitted unless such attachments have already been scanned for possible viruses and other malicious code.

### 3.1.8 Retaining or deleting Electronic mail (E-mail)

Data retention period for email must be established to meet legal and business requirement and must be adhered to by all staff.

## 4.0 INTERNET USAGE POLICY

### 4.1 Purpose and Scope.

#### 4.1.1 Definition

The objective of the internet usage policy is to protect the interests of the GoMC without inhibiting the use of the internet service that is intended for the greater benefit of staff members and GoMC at large.

These standards are designed to ensure that the internet is used in a safe and responsible manner. This policy applies to all GoMC staff, contractors, vendors and agents with GoMC-owned or personally-owned computer or workstation connected to the GoMC's network.

This policy applies to all end-user-initiated communication between the GoMC's network and the internet, including web browsing, instant messaging, file transfer etc.

#### 4.1.2 Internet Use Filtering System

The GoMC accepts no responsibility for consequential loss or damages arising from the use of its internet services for personal purposes.

ICT Directorate shall block access to internet websites and applications that are deemed inappropriate for GoMC's corporate environment. The following categories of websites (not exhaustive) shall be blocked: Entertainment, Adult/Sexual Explicit Material, Advertisements and Pop-ups, Gaming, Gambling, Hacking, illegal Drugs, Peer to peer file sharing, personal and dating, phishing and fraud, spyware, violence, intolerance and hate. ICT Directorate shall periodically review and recommend changes to web and content filtering rules.

#### 4.1.3 Use of Social Media

The ICT management shall determine from time to time the social media platforms to be accessed by staff at GoMC and enforce appropriate limitation.

#### 4.1.4 Unauthorized internet use

Includes but not limited to:

- Utilizing GoMC's Internet services to access, create, store or distribute pornographic materials.

- Running a business using the GoMC's internet services and facilities
- Installation or use of peer to peer file sharing programs such as Kazaa, Gnutella etc.
- Breaking any Law e.g. copyright infringement
- Video/Radio/Audio streaming as it consumes a lot of bandwidth.

### 4.1.5 Downloading Content from Internet.

Users are prohibited from downloading and installing software from the internet to the GoMC's computers. Users wishing to download software for installation should seek approval of the ICT Directorate.

### 4.1.6 Exemptions

The ICT Directorate will from time to time review the restrictions under sections 4.1.2, 4.1.3, 4.1.4 and 4.1.5 above. Any user who needs who needs to access restricted content for legitimate use should seek exemptions through the ICT Directorate in writing. Such exemptions, if granted, should not be misused.

### 4.1.7 Disruptions

The ICT Directorate endeavors to provide uninterrupted internet services at the highest level. However, disruption for administrative purposes and due to reason beyond the GoMC's control are unavoidable. In the event of internet service unavailability.

### 4.1.8 Using Internet for Work Purposes

ICT Directorate is responsible for controlling user access to the internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of information security incidents.

### 4.1.9 Use of Phones and Faxes

Staff making phone calls and using faxes are responsible for safe and appropriate use. Persons dispensed with the use of phones or faxes should exercise due-diligence.

## 5.0 NETWORK MANAGEMENT

### 5.1 Purpose and Scope

This policy defines how the GoMC network shall be configured and managed including the kind of personnel assigned this responsibility. It is the duty of the Accounting Officer to ensure adherence to this policy. The ICT Directorate reserves the authority over all GoMC Networks.

#### 5.1.1 Configuring Networks

It's the duty of the ICT Directorate to design, configure, manage and deploy networks in compliance with the approved standards, to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

Network addressing shall be centrally administered by the ICT Directorate.

#### 5.1.2 Accessing the Network Remotely

Remote access to the GoMC's network and resources shall only be permitted provided that authorized users are authenticated, data is encrypted across the network and privileges are restricted.

#### 5.1.3 Defending your Network Information from Malicious Attacks

Systems hardware, operating and application software, the networks and communication systems shall all be adequately configured and safeguarded against both physical attacks and unauthorized network intrusion.

#### 5.1.4 Time-out Facility

A time-out facility is to be provided to a network covering all terminals, servers and PCs to ensure that the screen are cleared and unauthorized access is prevented after a minimum time of inactivity.

#### 5.1.5 Authentication of Network Connecting Equipment

All users are prohibited from installing and/or plugging in equipment on the Network. Users seeking an exemption on this policy may seek approval from the ICT Directorate.

Users shall be assigned network accounts to access network resource including, but not limited to shared devices like printers and network storage. Such resources shall only be used for official purposes only.

### 5.2 System Operation and Administration

#### 5.2.1 Appointing System Administrators

The GoMC's systems shall be managed by suitably qualified systems administrators who are responsible for overseeing the day to day running operation and security of the Network systems.

#### 5.2.2 Administrating Systems

Systems administrators shall be fully trained and have adequate experience in the wide range of systems and platforms used by the organization. In addition, they shall be knowledgeable and conversant with the range of information security risk and risk management.

#### 5.2.3 Managing System Operation and System Administration

The GoMC's Systems shall be operated and administered using documented procedures in a manner which is not only efficient but also effective in protecting the organization's information security.

#### 5.2.4 Managing System Documentation

All documentation shall be kept up-to-date and be available.

#### 5.2.5 Monitoring Tools and Logs

Error logs must be properly reviewed and managed by qualified staff. Online monitoring tool to Networks systems must also be managed.

#### 5.2.6 Scheduling Changes to Routine Systems Operations

Changes to routine systems operation shall be fully tested and approved before being implemented.

#### 5.2.7 Responding to System Faults

Only qualified and authorized staff or approved third party technicians may repair information system hardware faults and give documentation of diagnosis.

## 6.0 INFORMATION AND DATA MANAGEMENT

### 6.1 Purpose and Scope

#### 6.1.1 Definition

This policy shall ensure that GoMC maintains a comprehensive and up-to-date database containing details of its data and information for the purpose of defining its value, criticality, sensitivity and legal implications. This policy covers all information users both internal and external, as well as that ICT staff charged with maintaining the database.

All digital data including but not limited to spreadsheets, databases and scanned copies shall be under the custody of the ICT Directorate. The Directorate is therefore responsible for the storage, backup, dissemination, securing and retrieval of the same data.

#### 6.1.2 Labeling Classified Information

All information, data and documents shall be clearly labeled so that all users are aware of the ownership, classification and value of the information. Suitable procedures are to be set up to provide control requirements and processing rules and regulations.

#### 6.1.3 Storing and Handling Classified Information

All information, data and documents shall be processed and stored strictly in accordance with the classification levels assigned to that information in order to protect its integrity, confidentiality, sensitivity, value and criticality.

#### 6.1.4 Accepting Ownership for Classified Information

The responsibility of each item of information, data and documentation shall be allocated to a specifically designated information owner or custodian.

#### 6.1.5 Managing Network Security

Access to information available through the GoMC's network systems shall be strictly controlled in accordance with approved access control criteria, which is to be maintained and updated regularly.

#### 6.1.6 Transferring, Exchanging, Managing and Archiving Data.

Sensitive or confidential information, shall only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured. Data storage must ensure that current data is readily available to authorized users and that archives are both created and accessible in case of need. Integrity and stability of GoMC's database shall be maintained at all times. Archiving of documents shall take place with due consideration for legal, regulatory and business issues. GoMC's information systems shall be retained for a minimum period that meets both legal and business requirements.

### 6.1.7 Sharing of Information

Employees are required to be fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organization and to external parties.

### 6.1.8 Sending Information to Third Parties and Other Stakeholders

Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but also the procedure and information security measures adopted by the third party shall be seen to continue to assure the confidentiality and integrity of the information.

### 6.1.9 Controlling Data Distribution

For authorized personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy.

### 6.1.10 Permitting Third Party Access

Third party access to corporate information shall only be permitted where the information in question has been safeguarded and the risk of possible unauthorized access is considered to be negligible.

## 7.0 ACQUISITION / PROCUREMENT OF ICTS

### 7.1 Purpose & Scope

This policy shall govern the acquisition and procurement, installation, maintenance and disposal of ICTs. This includes but not limited to ICT hardware and related peripheral, software, Telecommunication Equipment and ICT Consultancy services. ICT Directorate and IT steering committee and IT management committee shall ensure compliance to this policy.

### 7.2 PURCHASING AND INSTALLING ICTs

#### 7.2.1 Specifying Minimum Technical Specifications for ICTs

The purchase and installation of ICTs require those involved to consider carefully the technical standards involved in this process. This section covers the key areas to be considered. All purchases of new systems ICTs or new components for existing systems must be made in accordance with ICT Policy, as well as technical standards. Such purchase must be based upon a Minimum Technical Specifications document and/or TORs, SLAs and designs, and take account of long-term GoMC business needs.

The Minimum Technical Specifications document shall originate from the ICT Directorate and this shall be evaluated by the technical team appointed by the Accounting Officer.

Departments procuring ICTs shall consult with ICT Directorate to facilitate conformance to specifications and budget estimates.

The Directorate shall develop an ICTs requirement analysis document to map users at different levels to the appropriate ICT equipment.

During the budget making process, Departments shall consult the ICT Directorate before allocating ICT-related budgeting.

Based on the cost benefit analysis and value of the equipment to be purchased, the existing Public Procurement and Disposal Act rules shall apply.

#### 7.2.2 Installation and Deployment of ICTs

All new ICTs installations and deployment are to be planned formally and notified to all interested parties ahead of the proposed installation and deployment date. Prior communication will be circulated in advance to affected parties for all new installations and deployment.

Only ICT Directorate shall be responsible for the installation and deployment of ICTs throughout the County.

### 7.2.3 Testing Installed ICTs

All ICTs must be fully and comprehensively tested and formally accepted by ICT Directorate before being transferred to the live environment or user sites.

### 7.3 Supplying Continuous Power to Critical Equipment

Uninterruptible Power Supply is to be installed to critical equipment to ensure the continuity of services during power outages.

### 7.4 Use of ICTs

All GoMC staff are responsible for proper use and care of ICTs attached to them. Users are liable for integrity and security of information stored in their ICTs. This includes performing regular data back-ups and using up-to-date antivirus software protection.

### 7.5 Controlling IT Consumables

IT Consumables must be purchased in accordance with the GoMC's approved purchasing procedures with usage monitored to discourage improper use.

### 7.6 Working off Premises or Using Outsourced Services

Persons responsible for commissioning outsourced ICTs shall ensure that the services used are from reputable entity that operate in accordance with quality standards which should include a suitable service level agreement which meets the GoMC requirements.

### 7.7 Documenting ICTs

### 7.7.1 Managing and Using ICTs Documentation

All ICTs documentation shall be kept up-to-date and readily available to the staff who are authorized to support and maintain systems.

### 7.7.2 ICTs Inventory Support and Maintenance

A formal inventory of all ICTs shall be maintained and kept up-to-date at all times. It is the duty of the ICT Directorate to develop a periodic corrective and preventive maintenance schedule for all ICTs.

The ICT Directorate shall provide technical support to all departments upon request, or when deemed necessary in accordance with the technical support guideline.

### 7.8 Using Mobile Phones

Personnel issued with mobile phones by GoMC, or otherwise using mobile phones to conduct GOMC business, are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed.

### 7.9 Using Business Centre Facilities

Personnel using business centers to work on GOMC's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business center's systems.

### 7.10 Other Policies

#### 7.10.1 Disposal of ICTs

ICTs owned by GoMC shall only be disposed of by ICT personnel authorized by the ICT Directorate and ensure that the relevant security risks have been mitigated and this shall be in the line with the existing Public Procurement and Asset Disposal Act.

#### 7.10.2 Reporting and Recording Faults in ICTs

All faults of ICTs shall be promptly reported to the ICT Directorate for corrective action, and be recorded in a fault register.

#### 7.10.3 Insuring Hardware

Hardware needs to be adequately insured so as to enhance GoMC's resilience after a disaster.

All computing equipment and other associated hardware belonging to GoMC must carry appropriate insurance cover against hardware theft, damage, or loss.

All portable computing equipment is to be insured to cover travel domestically or abroad.

#### 7.10.4 Bring your own device policy

Staff shall not be allowed to bring in their personal ICTs to ride on GoMC ICT resources.

In the event that any staff may bring their own equipment and need to connect to the network, authority in writing shall be sought from the ICT Directorate, and this equipment / service shall be bound by this policy.

### 7.10.5 Moving Hardware from one Location to Another

This is the physical removal and relocation of hardware from one location to another.

Any movement of hardware between the different GoMC locations is to be strictly controlled by ICT Directorate. Personnel wishing to move ICT Equipment shall launch a formal request through the Directorate. Proper documentation should be maintained in the respective departments.

### 7.10.6 Maintaining ICTs (On-site or Off-site Support)

There shall be arrangements made for maintaining ICTs, whether through on-site or off-site support.

All GoMC ICTs shall be maintained and supported by ICT Directorate. Users shall not initiate or undertake maintenance of ICTs.

### 7.10.7 Damage to Equipment

Deliberate or accidental damage of GoMC equipment must be reported in writing as soon as it is discovered. Repair of any damaged equipment should be done by authorized personnel by the ICT Directorate.

### 7.10.8 Loss of Equipment

Loss of equipment shall be reported as soon as it is discovered. The lost equipment can pose a potential risk as it may contain highly confidential information.

Deliberate or accidental loss of, ICT related, GOMC equipment / property shall be reported to the ICT Directorate and other relevant authorities where necessary, as soon as it is noticed.

## 8.0 ICT CAPACITY BUILDING

### 8.1 Purpose & Scope

This Policy aims at enhancing the human and institutional ICT capacity to GoMC for improved service delivery through increased harmonization, coordination and management of ICT capacity building activities.

### 8.2 Community ICT Empowerment

The GoMC shall undertake, through the ICT Directorate, to periodically carry out ICT empowerment programmes to its citizenry, through GoMC ICT Centres or consultants or other stakeholders.

The Directorate shall develop training guidelines for the same.

### 8.3 Training of Staff

The ICT Directorate shall be responsible for the overall co-ordination of ICT capacity building programmes in the GoMC.

The Directorate shall develop/operationalize standards and regulations and carry out sensitization programmes.

Departments wishing to carry out ICT Related trainings shall present their request to the ICT directorate for action.

All ICT related trainings shall be coordinated by the ICT Directorate in collaboration with the relevant stakeholders.

This includes trainings that are part of the implementation of ICTs.

### 8.4 Training of ICT Staff

Every section within ICT department shall identify training needs every beginning of financial year and forward to the ICT Directorate.

The Directorate shall analyze the trainings relevant for every section to make sure that the training requirements are relevant to the various sections staff, within budget and implemented according to the ICT training guidelines.

### 8.5 Providing Regular Information Updates to Staff

GoMC is committed to providing regular and relevant Information Security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc.

### 8.6 Information Security Training on New Systems

GoMC is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security.

### 8.7 Training New Recruits in Information Security

All staff are to receive mandatory ICT Policy awareness training as part of induction.

## 9.0 ICT GOVERNANCE PROCESSES

### 9.1 IT Governance Processes

#### 9.1.1 Purpose & Scope

This policy spells out the IT governance structure of GoMC with emphasis on protection of IT resources, accountability for usage and compliance to the ICT policy by all system users.

#### 9.1.2 Protection of ICT Resources

All users of ICT resources at GoMC have a responsibility for protecting the security and integrity of both information and computer equipment.

The protection of all information system resources, such as computer systems hardware, application and systems software, data, documentation, and personnel, is a fundamental responsibility of all levels of management.

Departments must apply ICT standards to those IT assets under their management control. In particular, they must ensure that all ICTs that are critical to the operation of their business are adequately protected and that sensitive information handled by their staff is correctly classified and protected.

All Accounting Officers, at every level, are directly responsible for ensuring that all staff and contractors are aware of their obligation to safeguard GoMC's ICTs.

It is the responsibility of all members of staff to:

- Comply with ICT policy standards
- Act in a responsible and proactive manner regarding ICT security.

#### 9.1.3 Accountability for ICT Resources

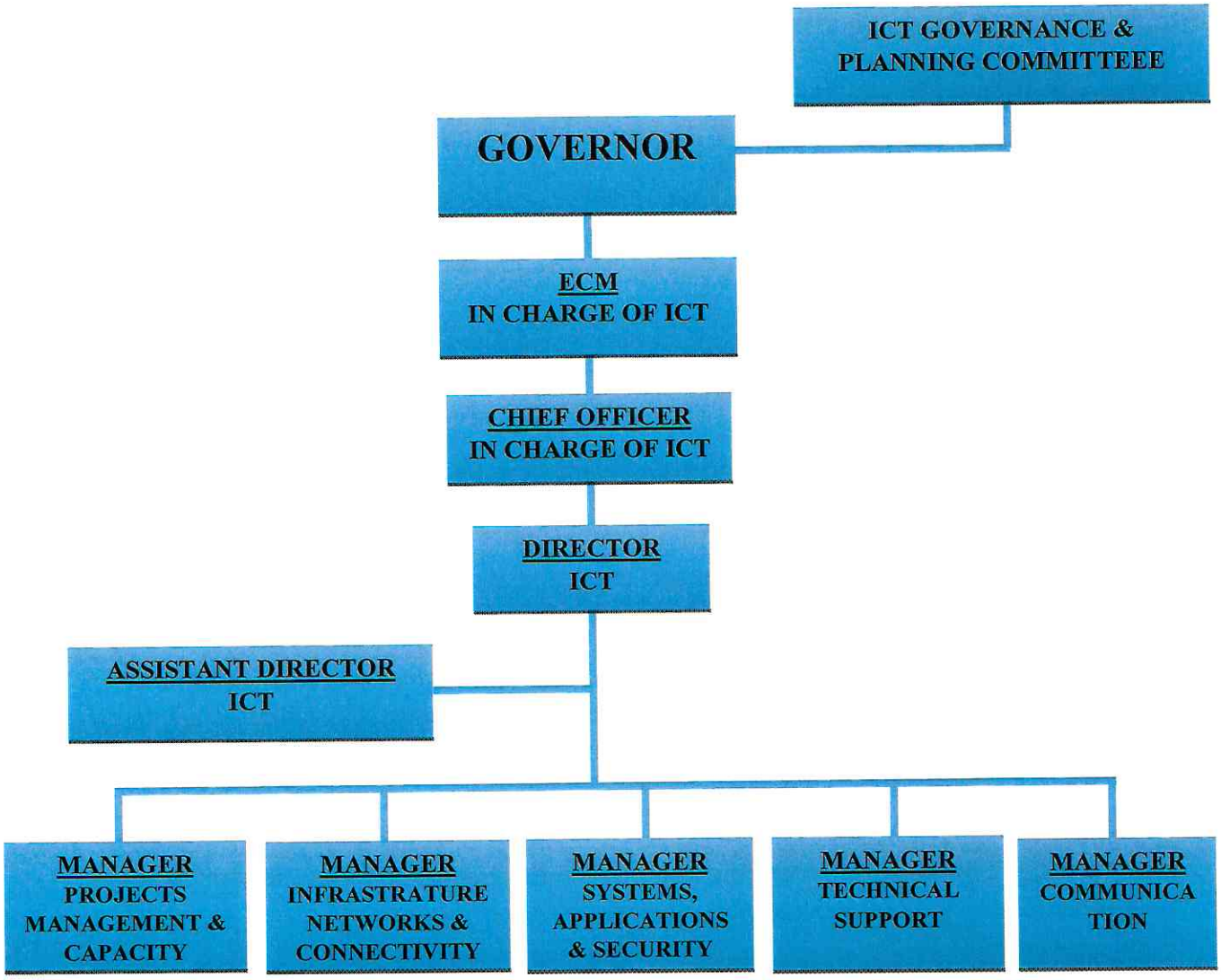
To ensure clear accountability, management should assign an owner to all assets (information, systems and equipment). Owners of information and systems are responsible for deciding what restrictions should be placed on the use of assets and authorizing access to the assets for those who have a business need.

A person who is responsible for ensuring that security standards are enforced will be designated at each GoMC site. This Local Security Focal Point will monitor security violations and direct corrective action with the ICT Directorate.

### 9.1.4 Compliance to ICT policy form

All staff, regardless of job function, will acknowledge in writing that he or she has read, understands and undertakes to comply with the ICT Policy attached to the user definition form which forms part of this policy.

### 9.2 ICT Governance Structures



## 10.0 CHANGE MANAGEMENT POLICY

### 10.1 Purpose & Scope

### 10.1.1 ICT Change Management Defined

ICT Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the ICT Infrastructure including the ICT Processes, Operating and Application Systems.

### 10.1.2 Basic Processes

The Change Management Process begins with the creation of a Request for Change (RFC). It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

### 10.1.3 Scope

The policy covers all planned and unplanned changes affecting the GoMC's information resources.

All changes-requests shall be logged, filtered/categorized and actioned by different levels of the ICT Management

### 10.1.4 Change Management

Every change to the GoMC's information resources under the scope of this policy shall be subject to Change Management and must follow the Change Management procedures outlined below. These procedures shall be subject to review.

- All emergency and unscheduled (unplanned) changes shall be documented once the changes have been effected. The change shall first be identified and classified as emergency.
- There shall be a formal independent analysis before changes are implemented
- All incidences must be logged and a report submitted to the ICT Directorate for record.
- All changes while adhering to the defined process shall be requested through the request for change control form
- All modification to the ICTs related systems shall be performed in such a manner to ensure continuity of the services supported by the system.
- Changes to the live (operating) environment that may disrupt services shall as far as possible be done outside business hours and shall ensure minimum disruption to dependent services.

- The business supporting function (within ICT) shall implement the change. The responsibility for the change in the IT environment (while maintaining segregation of duties) rests with the ICT Directorate.
- Project Team (PT) shall be appointed by the ICT Management to oversee the implementation of major changes in the ICT environment.
- Staff shall ensure that contractors and other service providers' work affecting information resource adhere to this policy and in accordance to the contractual agreements with GoMC. All contracts should refer to this policy explicitly.
- Stake holders to be affected directly or indirectly by the change should be informed through communication by the CEC Member in charge of ICT at least 24 hours before the change.

## 11.0 PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

### 11.1 Purpose & Scope

The purpose of this policy is to guide in the acquisition of commercial software that meets the user requirements and ensure compliance with legislation on software licensing. This policy shall be used by GoMC when acquiring commercial software.

#### 11.1.1 Specifying User Requirements for Software

All requests for new applications systems or software enhancements shall be presented to ICT Directorate with a Business Case with the business requirements presented in a User Requirements Specification document.

#### 11.1.2 Selecting Business Software Packages

The selection process for all new business software shall incorporate the criteria upon which the selection will be made. Such criteria shall receive the approval by the ICT Directorate.

#### 11.1.3 Using Licensed Software

To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements shall be strictly adhered to.

### 11.2. Software Maintenance & Upgrade

#### 11.2.1 Applying 'Patches' to Software

Patches to resolve software bugs may only be applied where verified as necessary and with ICT management authorization. They must be from a reputable source and are to be thoroughly tested before use.

#### 11.2.2 Upgrading Software

Upgrades to software must be properly tested by qualified personnel before they are used in a live environment

#### 11.2.3 Disposing of Software

The disposal of software should only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future date.

### 11.2.4 Acquiring Vendor Developed Software

Vendor developed software shall meet the User Requirements Specification and offer appropriate product support.

## 12.0 DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE

### 12.1 Purpose & Scope

The purpose of this policy is to guide in the development process of an in-house software for GoMC. It governs the software development process and incorporates software quality assurance measures so that the final product meets user needs. The business owners shall ensure compliance to this policy when developing in house software.

### 12.2 Software Development and Maintenance

Departments wishing to do systems development shall submit business case/ user requirements to the ICT Directorate. The Department will then analyze the scope in the business case in terms of viability, budget and mode of acquisition (in-house or out-sourcing) then advise accordingly.

The ICT Directorate shall in liaison with requesting department constitute a Project team for in-house development. The Directorate shall also determine the resource requirements to be provided by the requesting department, for a successful development and execution of the Project.

All in-house Development shall conform to the software standards of the directorate.

Any software developed in-house shall remain a property of GoMC, shall be governed by copyright laws and shall therefore not be used for any commercial purpose(s).

Departments shall not initiate or undertake any in-house development outside the above guidelines.

#### 12.2.1 Controlling Program Source Libraries and Old Versions of Programs.

Formal change control procedures with comprehensive audit trails are to be used to control Program Source Libraries and versions of old programs.

#### 12.2.2 Software Development

Software developed for or by the organization shall always follow a formalized development process which itself is managed under the project in question. The integrity of the GoMC's operational software code shall be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

#### 12.2.3 Making Emergency Amendments to Software

Emergency amendments to software shall be discouraged, except in circumstances previously designated by the relevant ICT Management as 'critical'. Any such amendments shall strictly follow agreed change control procedural rules.

### 12.2.4 Managing Change Control Procedures

Formal change control procedures shall be utilized for all amendments to systems. All changes to programs shall be properly authorized and tested in a test environment before moving to the live environment

### 12.2.5 Separating Systems Development and Operations

The relevant ICT Management shall ensure that proper segregation of duties applies to all areas dealing with systems development or systems administration

### 12.2.6 Capacity Planning and Testing of New Systems

New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organization

### 12.2.7 Documenting New and Enhanced Systems

All new and enhanced systems shall be fully supported at all times by comprehensive and up to date documentation before they're introduced to the live environment.

## 13.0 SECURITY

### 13.1 COMBATING CYBERCRIME

#### 13.1.1 Purpose & Scope

This policy shall govern how to mitigate the threats posed by cybercrime including denial of service attack and virus attack. It is the sole responsibility of ICT management to ensure compliance to this policy

#### 13.1.2 Defending Against Premeditated Cyber Crime Attacks

Security on the network shall be maintained at the highest level. GoMC, through the ICT Directorate shall invest on state-of the-art real-time network security Technology

#### 13.1.3 Minimizing the Impact of Cyber Attacks

The ICT Directorate shall prepare plans and maintain regular tests to ensure that damage done by possible external cybercrime attacks can be minimized and that restoration takes place as quickly as possible.

#### 13.1.4 Defending Against Premeditated Internal Attacks

In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards shall be periodically reviewed whilst maintained at all times.

#### 13.1.5 Safeguarding against Malicious Denial of Service Attack

Contingency plans for a denial of service attack shall be maintained and periodically tested to ensure adequacy.

#### 13.1.6 Defending Against Virus Attacks

Anti-Virus software shall be deployed across all PCs with regular Virus definition updates and scanning across all ICTs. It's the responsibility of the user to ensure that ICTs at their disposal run an Up-to-date antivirus by seeking assistance from the ICT Directorate

## 13.2 PASSWORD MANAGEMENT

### 13.2.1 Purpose and Scope

The purpose of this policy is to establish a standard for creation of strong passwords, protection of those passwords, and the frequency of change. Passwords are an important aspect of computer security. They are the frontline of protection for user accounts. A poorly chosen password may result in the compromise of the GoMC's entire network.

All employees and personnel that have access to the GoMC computer systems shall adhere to the password guidelines defined below in order to protect the security of the network and data integrity. These guidelines and procedures apply to any and all personnel who have any form of account requiring a password on the GoMC's network including but not limited to a domain and email account.

### 13.2.2 Password Protection

- Passwords must be kept confidential and not shared with colleagues. For departmental accounts, distribution lists to designated users accounts shall be created.
- Users are responsible for maintaining the security of their passwords.
- Users are responsible for all the activities performed with the account and therefore must not allow others to perform any activity with their usernames.
- It is recommended that you do not send a password through email or include it in a non-encrypted stored document.
- Always log out when you are not using your account.
- Report any suspicion of your password being compromised to the ICT Directorate in writing.

### 13.2.3 Password Change

Passwords must be changed under any one of the following circumstances

- After every 60 days (a must)
- Immediately, if a password has been compromised
- Immediately an account has been transferred to another user.

## 13.3 SAFEGUARDING ACCESS TO INFORMATION AND SYSTEMS

### 13.3.1 Purpose and Scope

This policy defines access controls to information and systems within GoMC. It covers access to the Operating system as well as access privileges granted to third parties. It further defines information ownership and access privileges to both internal and external users. It is the responsibility of ICT Directorate to ensure compliance to this policy.

### 13.3.2 Managing Access Control Standards

Access control standards for information systems shall be established in a manner that carefully balances restrictions to prevent unauthorized access against the need to provide unhindered access in accordance with the need of the business.

### 13.3.3 Managing User Access

Access to all systems shall be authorized by the nominated owner of that system and such access, including the appropriate access rights (or privileges) shall be of confidentiality, sensitivity, value of the data and be safeguarded accordingly.

### 13.3.4 Securing Unattended Workstations

Equipment is always to be safeguarded appropriately with password protected screen locks especially when left unattended.

### 13.3.5 Managing Network Access Controls

Access to the resource on the network shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

### 13.3.6 Controlling Access to Operating System Software

Access to operating system commands shall be restricted to those persons that are authorized to perform systems administration management functions. Such access shall be operated under dual control requiring the specific approval of the senior management.

### 13.3.7 Securing Against Unauthorized Physical Access

Physical access to high security area shall be controlled with strong identification and authentications techniques. Staff with authorization to enter such areas shall be provided with information on the potential security risks involved.

### 13.3.8 Restricting Access

Access controls shall be set at an appropriate level which minimizes information security risks yet also allows the GoMC's business activities to be carried without undue hindrance and record entrance.

### 13.3.9 Monitoring System Access and Use

Access is to be logged and monitored to identity potential misuse of systems or information.

### 13.3.10 Types of Access Granted to Third Parties

Access to systems, network and information shall only be granted to third parties in controlled circumstance and shall be approved based of type of access. The type of access would be either physical or logical and proper controls shall be applied to any such access granted.

### 13.3.11 Why Access is Granted to Third Parties

Access to system, network and information shall only be granted to third parties in controlled circumstances and shall be approved with clear reference to the reason why access is necessary.

### 13.3.12 Management Duties

Management has individual and collective responsibility to ensure third parties adhere to approved information security procedures.

### 13.3.13 Third Party Service management

Service level management concepts shall be applied to all deliveries of service from third parties. This will require third parties to meet all security and service controls, service definitions and agreed service level.

### 13.3.14 Monitoring Third Party Services

Third party service shall be governed through service level agreement and service level are to be monitored on an ongoing basis and penalty clauses invoked as appropriate.

### 13.3.15 Third Party Service Changes

Any changes that are to be made to service provided by third parties shall be agreed upon prior to the change taking place and the service level agreements amended accordingly.

## 13.4 PHYSICAL SECURITY

### 13.4.1 Purpose & Scope

This policy governs the physical protection of computer premises, environmental conditions and other external threats. The policy is alive to the fact that illegal physical access to ICTs can compromise the integrity of information and lead to loss of computer equipment as well.

### 13.4.2 Premises Security and Physical security

#### 13.4.2.1 Securing Physical Protection of Premises hosting ICTs

Premises **hosting ICTs** shall be safeguarded against unlawful and unauthorized physical intrusion using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts. Where necessary, security personnel maybe deployed

#### 13.4.2.2 Ensuring Suitable Environmental Conditions

When locating ICTs, suitable precautions shall be taken to guard against the environmental threats of fire, flood and excessive ambient temperature and humidity. The equipment must be protected from bad weather all the time.

#### 13.4.2.3 Environmental and other external threats

Appropriate safeguards against environmental and other external threats shall be applied to all premises to protect employees, sensitive information and other assets. These safeguards will be defined following a risk assessment and will be in keeping with the perceived risks and the nature of the assets being protected.

#### 13.4.2.4 Electronic Eavesdropping

Electronic eavesdropping shall be guarded against by using suitable detection mechanisms, which shall be deployed if and when justified by the periodic risk assessments at GoMC.

#### 13.4.2.5 Cabling Security

All cabling relating to ICTs shall conform to network standards as specified in the Network Cabling Document.

#### 13.4.2.6 Disaster Recovery Plan

Owners of the GoMC's ICTs shall ensure that disaster recovery plans for their systems are developed, tested, and implemented in consultation with the ICT Directorate.

## 13.5 ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY

### 13.5.1 Purpose & Scope

This policy recognizes the threats posed by internal & external users and defines compliance as a key condition for new staff and contractors.

It is the responsibility of HR and the Executive to ensure compliance to this policy requirement.

### 13.5.2 Contract Documentation

#### 13.5.2.1 Preparing Terms and Conditions of Employment

The Terms and Conditions of Employment of GoMC are to include requirements for compliance with ICT Policy.

#### 13.5.2.2 Contracting with External Suppliers / other Service Providers

All external suppliers who are contracted to supply ICTs to GoMC must agree to follow the ICT policies. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of ICTs, where necessary.

#### 13.5.2.3 Using Non-Disclosure Agreements (Staff and Third Party)

Non-disclosure agreements must be used in all situations where confidentiality, sensitivity or value of the information being disclosed is classified as proprietary.

#### 13.5.2.4 Complying with Information Security Policy

All staff shall comply with the ICT Policies of GoMC. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action.

#### 13.5.2.5 Staffs' Responsibility to Protect Confidentiality of Data

All staff are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with GoMC.

### 13.5.3 Personal Information Security Responsibility

#### 13.5.3.1 Sharing Organization Information with Other Employees

Confidential information should be shared only with other authorized persons.

#### 13.5.3.2 Signing for Work done by Third Parties

Only properly authorized persons may sign for work done by third parties.

#### 13.5.3.3 Ordering ICTs

Only ICT Directorate may order ICTs on behalf of the GoMC. These goods must be ordered in strict accordance with the existing Public Procurement and Disposal Act..

#### 13.5.3.4 Verifying Financial Claims and Invoices

All claims for payment of ICTs shall be properly verified for correctness and conformance before payment is effected.

### 13.5.4 Staff Leaving Employment

#### 13.5.4.1 Handling Staff on leave

Upon notification of staff **suspension or study leave**, Human Resources management shall consider with the ICT Directorate whether the member of staff's continued system access rights constitutes an unacceptable risk to the GoMC and, if so, take the necessary action.

#### 13.5.4.1 Handling Staff Resignations and Dismissal

Upon notification of staff resignations or dismissal, Human Resources management shall immediately notify the ICT Directorate to take the necessary action related to security.

#### 13.5.4.2 Completing Procedures for Terminating Staff or Contractors

Procedures are to be implemented for handling departing employees or contractors covering return of any ICTs in their possession and also controlling physical and logical access to sensitive information and assets.

#### 13.5.4.3 Third Party Contractor: Awareness Program

An appropriate summary of the ICT Policy shall be formally delivered to any such contractor, prior to any supply of ICTs, where necessary

#### 13.5.4.4 Providing Regular Information Updates to Staff

GoMC is committed to providing regular and relevant Information Security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc.

#### 13.5.4.5 Information Security Training on New Systems

GoMC is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security.

#### 13.5.4.6 ICT Staff Training

Periodic training for the ICT staff is to be prioritized to educate and train in the latest threats and Information Security techniques.

#### 13.5.4.7 Training New Recruits in Information Security

All staff are to receive mandatory ICT Policy awareness training as part of induction.

### 13.6 Network Security

All security issues related to network shall be implemented and in accordance to the Information Security standards and Network Standards.

### 13.7 Internet Security

GoMC shall endeavor to put in place appropriate security systems that can perform the following functions:

- Antivirus scanning – check for viruses, worms, Trojans etc. on all incoming and outgoing traffic.
- Intrusion detection and prevention systems – detect inappropriate, incorrect or anomalous activity against the network and enable the administrator to take appropriate action.

Content filtering – monitor and filter contents from the internet, chat rooms, instant messaging, e-mail and all other applications and report on violations identified.

### 13.8 Clear Screen Policy

With open plan offices becoming common you could accidentally expose confidential material. Information can be read from your screen, especially when your workstation is logged on and you are away from your desk. A Clear Screen Policy is an effective safeguard.

All users of workstations, PCs / laptops are to ensure that their screens are clear / blank when not in use.

## 14.0 COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

### 14.1 Purpose & Scope

This policy addresses compliance with the regulations governing use of ICTs such as the Communications Amendment Act of 2008. The objective is to avoid legal suits arising from abuse of ICTs. It is the responsibility of HR and The Executive to ensure compliance to this policy.

### 14.2 Complying with Legal Obligations

#### 14.2.1 Being Aware of Legal Obligations

The Human Resources Department is to ensure that all staff are fully aware of their legal responsibilities with respect to their use of ICTs. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organization Code of Conduct.

#### 14.2.2 Legal Safeguards against ICTs Misuse

The Human Resources Department is to prepare guidelines to ensure that all employees are aware of the key aspects of Computer Misuse in the Kenya Communications Amendment Act 2008 and the penal code legislation in so far as these requirements impact on their duties.

### 14.3 Complying with policy

#### 14.3.1 Complying with the ICT Policy

All staff are required to fully comply with the ICT policies. The monitoring of such compliance is the responsibility of ICT Management.

### 14.4 Avoiding Litigation

#### 14.4.1 Safeguarding against Libel and Slander

Staff are prohibited from writing derogatory remarks about other persons or organizations using GoMC ICTs.

#### 14.4.2 Using Copyrighted Information from the Internet

Information from the Internet or other electronic sources may not be used without authorization from the owner of the copyright.

### 14.5 Other Legal Issues

#### 14.5.1 Renewing Domain Name Licenses- Web Sites

Registered domain names, whether or not actually used for the GoMC's Web sites, are to be protected and secured in a similar manner to any other valuable asset of the organization

#### 14.5.2 Insuring Risks

A re-assessment of the threats and risks involved relating to the GoMC activities must take place periodically to ensure that the organization is adequately insured at all times.

## 15.0 RESPONDING TO INFORMATION SECURITY INCIDENTS & PLANNING FOR BUSINESS CONTINUITY

### 15.1 Business Continuity Plan

#### 15.1.1 Purpose & Scope

This policy governs the process of incident management and assigns responsibility of investigating security breaches. It also informs the process of initiating a BCP for prolonged incidents. It is the responsibility of The Executive and ICT management to ensure compliance to this policy.

#### 15.1.2 Planning for Disaster Recovery and Business Continuity

The ICT Directorate shall develop, test and implement a Disaster Recovery and Business Continuity Plan.

### 15.2 Disaster Recovery

This policy is intended to serve statutory goals pertaining to GoMC operations, data, and facilities. These include:

1. Ensure continuity of GoMC operations.
2. Protect safety and integrity of data.

GoMC through the ICT Directorate shall develop a disaster recovery plan that at least identifies and mitigates against risks to critical systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. The disaster recovery plan for information technology may be a subset of GoMC's comprehensive disaster recovery plan. The concept of a disaster recovery includes business resumption.

### 15.3 Backup Policy

#### 15.3.1 Purpose & Scope

The purpose of this policy is to define the process of data storage for protection, integrity and availability for future retrieval of GoMC's data in case of any catastrophe. The policy covers all system user's data stored in the workstations, laptops, servers and other portable devices.

#### 15.3.2 Backup Process

This procedure applies to all equipment and data owned and operated by GoMC.

The directorate shall implement a regular back-up of GoMC data, as per the stipulated backup guidelines.

Users must take regular backups of their key information on to the GoMC network in consultation with the ICT Directorate. Users are responsible for backing up their personal information.

## 16.0 LAPTOP MANAGEMENT POLICY

### 16.1 Purpose & Scope

This policy governs the use of Laptops assigned to GoMC staff for purposes of work. By receiving GoMC's laptop the user accepts responsibility for safeguarding it while it is signed out to them.

Laptops are tools provided by the GoMC for the sole purpose of GoMC's work. They remain GoMC's property and should be used for organization-related work. Once a staff member has been assigned a laptop, ownership and its accountability shall not be transferred.

### 16.2 The Policy

- The Laptop shall not be left in premises outside the GoMC, except where the assignee is performing GoMC's work.
- When leaving the workplace overnight, store the laptop in a locked drawer or cabinet.
- If you have a private office, close and lock the door if you leave during the day.
- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.
- If you are staying in a hotel, lock your laptop in a safe if your room has one. If no safe is available, lock your laptop in a suitcase when you go out.
- Keep the laptop in sight when going through airport checkpoints.
- If you are traveling by car, lock the laptop in the boot when you park.
- Do not use the computer in locations that might increase likelihood of damage or loss.
- Keep food and drinks away from the computer.
- Use a padded carrying case for the laptop.
- Always backup your work.

### 16.3 Reporting loss/theft or damage/faults

Report damaged or stolen equipment as soon as possible to ICT Directorate. Stolen laptop should also be reported to the police and an abstract obtained.

If the laptop is stolen during an assault, or if it is damaged or stolen despite you having followed the guidelines listed above, it will be replaced. However, if the laptop is damaged or stolen and the above procedures were not followed, you shall be liable.

### 16.4 Using Laptop/Portable Computers

Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating portable computing facilities and implement the appropriate safeguards to minimize the risks

### 16.5 Working from Home or Other Off-Site Location

Off-site computer usage, whether at home or at other locations, shall only be used with the authorization of ICT Directorate.

Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.

### 16.6 Day to Day Use of Laptop / Portable Computers

Laptop computers shall be issued to, and used only by, authorized employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.

### 16.7 Replacement of Laptops

If the laptop is stolen during an assault, or if it is damaged or stolen despite the user having followed the guidelines listed above, it shall be replaced.

However, if the laptop is damaged or stolen and the above procedures were not followed, the user shall be liable.

Laptops will be deemed to be obsolete after 4 years of continuous use and the same replaced upon re-evaluation by the directorate of ICT.

## 17.0 POLICY COMMUNICATION, MONITORING AND EVALUATION

### 17.1 Communication

The county shall endeavor to continuously disseminate the provisions of this policy to all stakeholders using appropriate channels.

### 17.2 Monitoring & Evaluation

For successful implementation of the ICT policy, an M&E framework will be developed as an integral component to ensure the policy objectives are achieved in a cost effective, coordinated and harmonized approach at both the National and County levels. The department in charge of Education & ICT with the relevant implementing Departments and other relevant stakeholders will develop this framework within six months of the policy implementation.