Preface

The Teachers Service Commission has actively participated in the implementation of the wider Government of Kenya development policies that embrace the Public Service Reform Programmes and implementation of the Vision 2030 Strategy among others. In this regard, the Commission has set up internal structures to manage the reform initiatives necessary to enhance efficiency and effectiveness in teacher management in the country. This has been done in keeping with its Vision Statement “To be an institution of excellence in the provision of effective service for quality teaching”

The Teachers Service Commission (TSC) initiated its first computerization project with the implementation of the Education Management Information System (EMIS) in collaboration with the Ministry of Education in 1999. Since then, it has consistently developed systems to automate various functions in the service areas. These systems include the Integrated Personnel Payroll Database (IPPD), the Integrated Financial Management Information System (IFMIS) and the on-going development of the File Tracking system.

However, the Commission acknowledges the fact that it has not been able to keep pace with technological advancements in service delivery. The field of ICT has become more complex and dynamic, both in terms of technologies available and skills required. The Commission has all along operated without an explicit ICT policy to guide its capacity utilization and address the emerging issues in this field.

The Challenge for the Commission is therefore to develop a clear vision and an appropriate implementation plan that will anticipate technological changes and identify ICT opportunities outside the traditional work practices. The development of this policy has
therefore become a priority if the Commission is to realize the benefits that ICT promises.

This Policy has made an effort in customizing public sector ICT guidelines and procedures and establishes institutional structures that will integrate the use of ICT in the Commission’s operations for effective service delivery. The policy has also incorporated and amplified the aspirations of the Vision 2030 Strategy in ICT.

It is my belief that this policy, together with the accompanying ICT Strategy and structure will address the operational gaps that have existed and eventually transform the Commission to a knowledge based institution of excellence in the education sector.

Ibrahim Hussein, EBS, HSC
Chairman, Teachers Service Commission
Foreword

The objective of the ICT Policy is to guide the mainstreaming of ICT in the Teachers Service Commission. It has been developed in acknowledgement of the growing importance of ICT in supporting operations in the Commission. The Policy aims at achieving efficiency and effectiveness accruing from the application of ICT, and ultimately improving service delivery. It is built on three pillars: Information Systems, Information Technology and Human Resources.

The concept of ICT starts with policies relevant to information systems that support all service areas, which are the basis for fulfilling the mandate of the Commission. This policy provides guidelines on integrating the information systems within the Commission for improved service delivery.

Information Technology is essential in ensuring that information systems operate as expected with the human resource acting as a catalytic ingredient that determines how systems perform and assist the Commission in the discharge of its mandate. The people further develop, operate and manage information systems and information technology resources. Together these elements form the central theme of the ICT policy the Commission has developed.

However, this policy goes beyond these elements in two important ways. First, it seeks to ensure that these essential elements are safeguarded and, secondly, that there is a recovery strategy in the event of failure. It is for this reason that the ICT Policy contains strong elements on security and business continuity policies.

The responsibility to ensure that the policy is effective lies with each of one us individually and collectively. The management on
its part will play its role by ensuring each one of us is aware of its existence.

The Commission will publish the ICT Policy on its website, intranet and in hard copy, which shall be developed and updated annually by the ICT Steering Committee.

Gabriel K. Lengoiboni, EBS
Secretary/Chief Executive
Teachers Service Commission
TABLE OF CONTENTS

Preface........................................................................................................................................... i
Foreword ........................................................................................................................................ iii
TABLE OF CONTENTS ......................................................................................................................... v
ACRONYMS ..................................................................................................................................... vi
Definition of Terms ........................................................................................................................... vii
Part I: Introduction................................................................................................................................. 1
  1.0  Introduction .................................................................................................................................. 1
      1.1  Background ................................................................................................................................. 1
      1.2  Rationale ................................................................................................................................... 2
      2.0  Policy Statement ......................................................................................................................... 3
  3.0  Authority..................................................................................................................................... 3
  4.0  Vision, Mission and Objectives of the ICT Policy ........................................................................ 5
      4.1  Vision Statement ........................................................................................................................... 5
      4.2  Mission Statement ....................................................................................................................... 5
      4.3  Objectives of the TSC ICT Policy ................................................................................................. 5
  5.0  Scope .......................................................................................................................................... 6
  6.0  Key Principles ............................................................................................................................... 6
  7.0  Roles and Responsibilities ......................................................................................................... 6
  8.0  Part II - Information Systems Policies ....................................................................................... 7
      8.1  Information Systems ..................................................................................................................... 7
      8.2  Data Management ....................................................................................................................... 9
      8.3  Internet Based Systems .............................................................................................................. 10
  9.0  Part III - Information Technology Policies ................................................................................ 11
      9.1  Information Technology ............................................................................................................ 11
      9.2  Procurement .............................................................................................................................. 12
      9.5  Operation ................................................................................................................................ 12
      9.7  Decommissioning of ICT equipment ........................................................................................ 13
      9.8  Disposal ................................................................................................................................... 13
  10.0  Part IV- ICT Human Resources Development Policies ............................................................ 14
       10.1  Objectives .............................................................................................................................. 14
       10.2  ICT Governance .................................................................................................................... 14
       10.3  Capacity building ................................................................................................................... 14
  11.0  PART V- System Controls and Security Policies ....................................................................... 15
       11.1  Objectives .............................................................................................................................. 15
       11.2  Systems Security Control Policy ............................................................................................ 15
       11.3  Physical Security ..................................................................................................................... 16
       11.4  Passwords ............................................................................................................................... 16
       11.5  Data Security ........................................................................................................................... 16
       11.6  Copyright and license agreements ......................................................................................... 16
       11.7  Internet .................................................................................................................................. 16
       11.8  Email ...................................................................................................................................... 17
  12.0  PART VI- BUSINESS CONTINUITY POLICIES ................................................................. 17
       12.1  Responsibilities of the Commissioners and Top Management ............................................. 17
  13.0  Monitoring And Evaluation ....................................................................................................... 20
       14.0  Policy Review ........................................................................................................................ 20
ANNEX I: POLICY IMPLEMENTATION GUIDELINES .............................................................. 21
ANNEX II: ACKNOWLEDGEMENT OF ICT SECURITY POLICY ........................................ 34
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Assessment</td>
</tr>
<tr>
<td>EMIS</td>
<td>Education Management Information System</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resource</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication &amp; Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Identity</td>
</tr>
<tr>
<td>MCA</td>
<td>Mission Critical Activities</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objectives</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SDSCA</td>
<td>Senior Deputy Secretary (Audit)</td>
</tr>
<tr>
<td>TSC</td>
<td>Teachers Service Commission</td>
</tr>
</tbody>
</table>
Definition of Terms

**ICT (Information and Communication Technologies):** ICT means technologies, including computers, telecommunication and audiovisual systems, that enable the collection, processing, transportation and delivery of information and communications services to users.

**A Vision Statement:** A *Vision statement* outlines what an organisation aims to be. It concentrates on future; it is a source of inspiration. An ICT Vision statement defines where the organization wishes to be in relation to application of ICT to its business.

**ICT Mission:** A *Mission statement* is a general statement of the overall purpose and aims of the ICT policy and strategies. It concentrates on present; it defines the customer(s), critical processes and the desired level of performance. It is a progressive roadmap towards the attainment of a vision.

**ICT Policy:** A *policy* is a deliberate plan of action to guide decisions and achieve rational outcome(s). Policy differs from rules or law. While law can compel or prohibit behaviours (e.g. a law requiring the payment of taxes on income) policy merely guides actions toward those that are most likely to achieve a desired outcome.

**ICT System:** An ICT system definition includes, but is not limited to, hardware, software and communications equipment that the Commission uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance.
**User:** A user means any person who is recognized by the Commission as having a valid reason to access the Commission ICT systems whether that access is from within the Commission or outside the Commission.

**Alternate Site:** Alternate Site means a site held in readiness for use in the event of a major disruption that maintains an organisations’ business continuity.

**Business Continuity:** It is a state of continued, uninterrupted operation of a business.

**Business Continuity Management:** It is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.

**Business Continuity Plan:** This means a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

**Business Impact Analysis:** This means the process of identifying, and measuring (quantitatively and qualitatively) the business impact loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements and essential staff and to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.

**Call Tree:** It means a system that enables a list of persons/roles/organizations to be contracted as part of an information/communication plan.
**Communication Protocols:** This means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.

**Critical Services:** It means any activity, function, process or service, the loss of which would be material to the continued operation of a financial institution.

**Crisis:** It is an event, occurrence and/or perception that threaten the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an institution.

**Crisis Management Team:** It means a team consisting of key executives, key role players (i.e. legal counsel, facilities manager, disaster recovery coordinator), and the appropriate business owners of critical functions who are responsible for recovery operations during a crisis. Evaluation of capability, training, testing of Crisis Management teams maturity level must be documented.

**Disaster:** This is a sudden, unplanned catastrophic event that compromises an organization’s ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.

**Emergency Response Team:** It’s any organization that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals)

**Exercising:** This is the process through which business continuity plans are tested and rehearsed in a controlled environment using team members and staff.
Major Operational Disruption: It is a high impact disruption of normal business operations, affecting a large geographic area and adjacent communities that are economically integrated to it.

Operational Risk: It means the risk of loss from inadequate or failed internal processes, people and systems or from external events.

Recovery: This is the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

Recovery Objective: This means a predefined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).

Recovery Time Objective (RTO): Means the duration of time required to resume a specified business operation. It has two components, the duration of time from activation of the business continuity plan and the recovery of business operations.

Recovery Point Objective (RPO): Recovery Point Objective describes a point in time to which data, must be restored from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption.

Resilience: Means the ability of an organisation, network, activity, process or financial system to absorb the impact of a major operational disruption and continues to maintain critical operations or services.

Risk Assessment: It means the probability and impact of specific threats being realised.
**Single Point of Failure:** It is a unique source of a service, activity, and/or process where, there is no alternative and whose loss could lead to the failure of a critical function.

**Administrators** - Person responsible for management of a particular aspect of ICT resources

**Manager/ Supervisor:** Person overseeing overall ICT resources in managing access rights and work allocation.

**User:** Any person authorised by way of access rights to use an ICT resource.

**Portal:** An organisation’s data/information resource accessed via internet for public usage.
Part I: Introduction

1.0. Introduction

The Information Communication Technology (ICT) division provides regular, timely and accurate data and information for the purposes of policy formulation, planning and evidence-based decision making on staffing and establishment. Specifically, EMIS data is critical for decision making on staffing and planning issues. The division also administers TSC website, Local Area Network (LAN) at headquarters and provides internal ICT training. The division also provides specific technical services to all divisions at headquarters and the requisite ICT services user support by way of trouble-shooting and limited maintenance services.

Additionally, the division provides technical support to the Human Resource Division in regards to the implementation of the Integrated Personnel Payroll Database (IPPD) system for both the Secretariat and teachers and the integrity division on the development and maintenance of the inventory on wealth declaration information. In instances where the Commission is required to procure and install ICT equipment and software, the division provides technical advice in terms of technical specifications and subsequent inspection of the equipment and software procured. The division also liaises closely with MOE in ICT matters that relate to the wider education sector.

1.1 Background

In 2005, the Commission adopted a five-year Strategic Plan that outlined its overall vision, mission as well as other ways to improve delivery of services. One of the areas that the
Commission is giving considerable attention is the formulation and implementation of an ICT policy and strategy.

The Commission is aware that most institutions in both the public and private sectors are re-defining their policies and strategies to embrace ICT. In the public sector for example, the e-government strategy and the National ICT Policy were adopted in 2004 and 2006 respectively. The Ministry of Education Strategy for ICT was later launched in 2006. The overall objective of the above policies being to improve service delivery in keeping with 21st century challenges.

The immediate challenge for Commission is to establish medium and long-term ICT plan and adoption of an enabling policy. There is also need to harmonize and integrate existing systems, present and future initiatives. In this regard efforts to establish appropriate ICT standards, data security systems and procedures as well as related quality assurance mechanisms are a priority. In addition the Commission will need to address organization re-engineering, related staffing issues and ICT staff development.

1.2 Rationale

ICT capacity in TSC has grown as demonstrated by the number of equipment and the personnel who have received basic, functional and specialized training. ICT infrastructure has also been improved by the installation of a Local Area Network at the headquarters.
The current challenges being experienced by ICT service area are occasioned by the level of existing capacity in terms of technology, centralization of the information systems at the headquarters, lack of information systems integration, state of facilities and infrastructure at district offices. The service objective is to increase the capacity of TSC Headquarters and field offices to access data and process information necessary for improved service delivery. It is also envisaged that operations at TSC Headquarters will be automated and interconnectivity between TSC and other relevant organizations will be achieved.

2.0 Policy Statement

The Commission will continuously enhance its organizational capacity by adopting modern technology and skills development. This policy will ensure that ICT resources are optimally utilized in order to achieve efficiency in service delivery. It will facilitate efficient and effective service delivery through timely provision of a robust ICT infrastructure, application software, support services and operational capacity.

3.0 Authority

The policy derives its authority from:

(i) TSC Act Cap 212 of the Laws of Kenya;
(ii) The Code Of Regulations for Teachers and Secretariat Staff;
(iii) E-Government Strategy;
(iv) National ICT Policy;
(v) The Freedom of Information Bill; and
(vi) Any other relevant legal provision that may come into force
4.0 Vision, Mission and Objectives of the ICT Policy

4.1 Vision Statement

“To be knowledge based institution of excellence in the education sector”.

4.2 Mission Statement

“To mainstream the use of ICT in the Commission’s operations for improved service delivery”.

4.3 Objectives of the TSC ICT Policy

The objectives of TSC’s ICT policy are to:

(i) Support the development and implementation of ICT in the Commission;
(ii) Ensure development and maintenance of ICT systems;
(iii) Promote efficient and effective operations and usage of ICT systems within the Commission;
(iv) Facilitate the development of ICT skills to support ICT systems in the Commission;
(v) Encourage innovations in technology development, use of technology and general work flows within the Commission;
(vi) Promote Information sharing, transparency and accountability within the commission and towards the general public;
(vii) Promote efficient communication among the Commission’s staff and stakeholders; and
(viii) Ensure that ICT facilities are fully accessible to users with special needs; and
(ix) Ensure that ICT facilitates are gender responsive.
5.0 Scope

The ICT Policy shall apply to all the Commission’s employees and stakeholders including Agents. The policy will address Information Systems, Information Technology, Human Resource Development, Governance and Business Continuity strategies in relation to the Commissions operations.

6.0 Key Principles

This policy shall be guided by the following key principles:

(i) Mainstreaming of ICT in the Commission;
(ii) Seamless integration of ICT;
(iii) Inclusion, flexibility and support of other quality management systems;
(iv) Adherence to best practices & policies;
(v) Economies of scale and customer value propositions.

7.0 Roles and Responsibilities

The overall responsibility of implementing this policy will lie with the Commission Secretary in collaboration with ICT Governance Committee which will be responsible for the overall strategic management of ICT resources in the Commission. The Committee will draw representation from heads of departments and the head of ICT will be secretary. Specifically, the Committee will be responsible for oversight, enforcement and review of the policy and the initiation of ICT projects.
8.0 Part II - Information Systems Policies

8.1 Information Systems

Information Systems policies are intended to support structured approach to acquisition, development, operations and maintenance of information systems in the Commission. In this way, the Commission will guarantee their success and, therefore better decision support to meet its mandate. The head of ICT is the sole custodian and technical administrator of all Information Systems and Applications in the commission.

8.1.1 Application Systems

8.1.1.1 Initiation of a Software Project

All software acquired and developed shall be used strictly for TSC purposes only. Every software acquisition or development request shall be initiated through a written statement of scope and objective. The written statement will be submitted to the Commission ICT Governance Committee.

8.1.1.2 Acquisition

With respect to software acquisition:
(i) The Commission will use packaged software as the preferred option;
(ii) In the event that custom development of software is proposed, the request for such development must be justified on case by case basis;
(iii) Only open source software with technical support shall be used with approval by the head of ICT.

8.1.1.3 Development

With respect to software application development:
(i) Each software development project will be initiated on the basis of an approved requirements specification which:
   a. Identifies user requirements (functional requirements) expressed in non-technical language;
   b. Provide return on investment analysis; and
   c. Identifies beneficiaries.

(ii) If the Requirements (specifications) are approved the project sponsor and owner will proceed with the technical Specification to express user requirements specified in technical language
(iii) The TSC shall purchase only fully licensed copies of computer software;
(iv) User testing and acceptance are the necessary and sufficient conditions
8.1.4 Maintenance

Application software maintenance is critical for effectiveness and efficiency of the system. The following policy will therefore apply:

(i) Access to live systems will be restricted to authorized users;
(ii) Application software purchased must have service level maintenance agreements to ensure continuity;
(iii) Only certified or supplier authorized agents will be allowed to provide maintenance;
(iv) Internal maintenance shall be provided by personnel trained and certified; and
(v) Maintenance contracts for Information systems in the Commission shall be managed by the head of ICT.

8.1.5 System Decommissioning

With respect to systems decommissioning:

(i) All systems that will be commissioned shall have a predetermined life span;
(ii) At the end of the system life span, a review shall be done for the purpose of determining system usage, continuity or discontinuity;
(iii) For systems that have been in existence for five (5) years and above, a comprehensive review shall be carried out immediately this policy is effective;
(iv) For all newly acquired systems, a post installation review shall be carried out six (6) months after commissioning while subsequent reviews will be undertaken every two (2) years;
(v) Systems that are no longer effective or in use will be decommissioned within 6 months after the review.
(vi) A Decommission Certificate will be issued on successful conclusion of the exercise;
(vii) Existing software will be replaced in the presence of a Certified Information Systems Auditor;
(viii) All copies of existing systems and data shall be placed in protective custody of the head of ICT for at least 15yrs.
8.1.2 Operating systems

The following policies are intended to facilitate the governance of office automation within the Commission:

(i) Microsoft’s Windows Operating Systems will be the preferred Operating System for all computers.
(ii) The Commission will standardise its office productivity tools on the Microsoft Office suite;
(iii) Commonly used functions that require the same templates will be supported through issuance of Commission-specific templates.

8.1.3 Anti-virus software

With respect to anti-virus software:

(i) The head of ICT shall ensure availability and continuous update of anti-virus protection on all computers, laptops and servers;
(ii) No person shall be allowed to connect private PCs, laptops, modems or any ICT peripheral to commission’s network or hardware; and
(iii) All removable media in use within the Commission must be scanned for viruses.

8.2 Data Management

In order to ensure that data and information are available as and when required, the following policies will be adopted:

(i) It is the responsibility of heads of functional areas in close consultation with the head of ICT to determine and design the data that should be available in the Commission.
(ii) The head of ICT will ensure overall data capture, availability, accuracy, confidentiality, and integrity.
(iii) The Commission will acquire systems and tools to create, process, manage and preserve data;
(iv) The data shall be classified into Confidential and Public.
8.3 Internet Based Systems

The head of ICT will adopt and develop the following internet based systems as a means of communication and service delivery:

(i) Web sites;
(ii) E-mail systems;
(iii) Short Message Services;
(iv) Intranet; and
(v) Collaborative systems.
9.0 Part III - Information Technology Policies

9.1 Information Technology

The objectives of Information Technology policies must be consistent with public sector standards issued by relevant authority such as the Public Procurement Authority and E-Government Secretariat.

9.1.1 Desktop Computers

(i) The Commission shall seek to:
   (a) Standardize hardware equipment to minimize multi brands;
   (b) Allocate computers to user departments appropriately;
   (c) Provide uninterrupted power supply and protection to all ICT installations in order to protect the systems from power fluctuations and surges; and
   (d) Review hardware specifications to be in line with current technological trends.

(ii) Users are accountable for all ICT equipment allocated to them.

9.1.2 Laptops

With respect to Laptops:

(i) Laptops will be procured for service areas and assigned to officers whose nature of work merits their use;
(ii) Hardware specifications will be reviewed to be in line with current technological trends;
(iii) Users are accountable for all laptops issued to them; and
(iv) There will be no additional software installation without prior authority from the Head of ICT.

9.1.3 Servers

The following best practices will be adhered to with respect to server deployments within the Commission:

(i) Maximization of the storage system;
(ii) Ensuring online and offsite backups and real-time replication for critical applications;
(iii) Disaster prevention arrangements (see Business Continuity);
(vi) The acquisition of servers should be standardised to avoid multi brands;
(vii) All servers other than for backing up and disaster recovery shall be located in a central server room;
(viii) The head of ICT will be responsible for the administration of all the servers in the TSC;
(ix) Provide uninterrupted power supply and protection for all servers; and
(x) Review hardware specifications to be in line with current
technological trends.

9.2 Procurement

The procurement of hardware, software, peripherals and network products shall be guided by procurement laws and regulations and:

(i) Must conform to minimum specifications and standards established by the head of ICT;

(ii) Must be informed by annual procurement plans.

(iii) Take into account software requirements and anticipate future requirements;

(iv) The C.E.O will approve directly procurement of ICT emergency equipment.

(v) Be from manufacturers, authorised dealers and/or certified service centres.

(vi) Must have warranty.

9.3 Inventory

i. The Commission shall establish and maintain an inventory of all ICT equipment in the service areas.

ii. In the event of movement of officers occasioned by deployment or exit, the head of the affected service area shall reallocate any ICT equipment under their custody and communicate the same to the head of ICT, for purposes of updating the inventory.

iii. Movement of ICT hardware from one office to another is restricted.

9.4 Installation

On installation of information technology products:

(i) An Installation Certificate must be issued and signed by the head of ICT who shall be involved in the entire installation process;

(ii) The head of the service area shall be responsible for all installations; and

(iii) All installations must be in accordance with the supplier standards and Commission requirements;

9.5 Operation

(i) All operations must have User and Technical manuals from the supplier;

(ii) The operating environment must conform to the minimum manufacturers’ specifications or international standards; and

(iv) Emergency procedures must be clearly displayed in the server room and data centre.
9.6 Maintenance of ICT equipment

Maintenance of ICT equipment is critical for effectiveness and efficiency of TSC operations. The following policy will therefore apply:

(i) ICT hardware purchased must have Service Level Maintenance Agreements on expiry of the warranty;
(ii) Only certified manufacturer authorized agents will be allowed to provide maintenance; and
(iii) Internal maintenance shall be provided by personnel trained and certified.
(iv) Maintenance contracts for ICT equipment shall be managed by the head of ICT.

9.7 Decommissioning of ICT equipment

With respect to decommissioning ICT equipment:

(i) All ICT equipment shall have a predetermined life span;
(ii) There must be written justification by the head of ICT for decommissioning of any ICT equipment;
(iii) Equipment that are no longer effective or in use will be decommissioned within 6 months after the review;
(iv) ICT equipment will be decommissioned after an installation certificate has been issued for replaced systems;
(v) A Decommission Certificate will be issued on successful conclusion of the exercise.

9.8 Disposal

Information technology resources disposal must:

(i) Be in accordance with the existing public disposal rules and regulations;
(ii) Avoid or minimize degradation to the environment;
(iii) Seek to re-use some of or all the computer components;
(iv) Seek authority to donate any retired computer equipment;
(v) Remove data and systems on all hardware to be disposed off;
(vi) Comply with manufacturer, supplier or service provider terms and conditions of disposal; and
(vii) Be indicated on the Disposal Certificate.

---

1 Currently, the operating Public Procurement policies and procedures guided by the Public Procurement and Disposal Act 2005.
10.0 Part IV- ICT Human Resources Development Policies

10.1 Objectives
The human resource aspect of ICT is to ensure that the Commission has personnel who are able to:

(i) Provide effective and efficient support in the development and maintenance of ICT;
(ii) Use ICT to support efficient and effective service delivery;
(iii) Innovate and apply new technology consistent with ICT trends.

10.2 ICT Governance

(i) Structure of the TSC ICT Governance
   a. The ICT function shall operate as a department as per the proposed structure in Annex III.
   b. End user departments will be responsible for data input and operations of the departments’-specific systems.

(ii) The ICT Governance Committee
   A permanent ICT Governance Committee shall be established with the responsibility of the overall strategic management of ICT resources in the Commission. The Committee will be chaired by the Commission Secretary. The members will include heads of departments and the head of ICT as its secretary.

(iii) Specific responsibilities for the ICT Governance Committee will include
   a. Recommending, overseeing enforcement and reviewing the overall TSC ICT policy;
   b. Providing direction and oversight in the implementation of the ICT strategy; and
   c. Initiating and monitoring the implementation of ICT projects.

10.3 Capacity building
With respect to capacity building:

(i) The head of ICT will be responsible for the determination of overall ICT training needs and capacity building for TSC employees and agents;
(ii) The Commission will provide all employees with ICT skills and capabilities necessary for use of ICT resources;
(iii) A skills development programme consistent with the overall and strategic plan and Human Resource Development policy will be developed and implemented.
11.0 PART V - System Controls and Security Policies

The Commission has invested substantially in ICT resources. These resources are vital in realizing the Commission’s business objectives and are integral to the ability of the Commission to operate effectively. This policy establishes general guidelines, rules and regulations for the use and protection of the Commission’s information and ICT systems.

The implementation of this policy will thus promote the availability, integrity and confidentiality of the Commission’s ICT systems.

11.1 Objectives

The objectives of system controls and security policy are to:

(i) Create general awareness on appropriate security measures that must be implemented to safeguard the effective operation of the Commission;
(ii) Communicate the responsibilities for the protection of ICT systems;
(iii) Facilitate the preservation of the integrity and privacy (confidentiality) of the Commission’s information and
(iv) Protect and promote the Commission’s reputation.

11.2 Systems Security Control Policy

The Commission’s ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organisation, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved;

(i) Access
Access to the systems will be restricted to authorized users as determined by the head of a service area.

(ii) Breaches
Any breach of this policy shall be dealt with under the Commission’s Disciplinary Policy and Procedures. In addition, the Commission may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed.

(iii) Review
The Commission will establish the ICT Security Committee whose responsibilities will include the review of this aspect of the ICT policy at intervals of six (6) months and amended as need arises. Any changes shall be communicated to all users of the Commission’s ICT systems.
11.3 Physical Security

ICT resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability the Commission will institute appropriate control measures to ensure that its ICT resources are safeguarded.

Appropriate controls will be established to limit access to ICT infrastructure, computer equipment and data, commensurate with the acceptable level of risk. The access to the Commission’s ICT systems shall be reviewed every six (6) months.

11.4 Passwords

The ICT department shall prevent unauthorized access to the Commission’s corporate computer systems. Such controls shall take the form of passwords in the user identification process.

11.5 Data Security

The head of ICT shall develop rules, regulations and guidelines that ensure confidentiality, integrity, availability and safety of all Commission information.

11.6 Copyright and license agreements

Only licensed software shall be used in the Commission. Copying and distribution should not be done without the necessary licenses. The head of ICT department will ensure that all software applications used by the Commission complies with the relevant licensing agreements, compile all relevant licensing agreements and maintain a record.

11.7 Internet

a. To ensure productive, appropriate use and to minimize risks, access to the Internet should be limited to staff who need it for their work. Users should use the Internet in an effective, ethical and in a lawful manner.

b. Users should not use the Commission’s Internet access to view, print, distribute, display, send or receive images, text or graphics of offensive or obscene material or material that violates any Kenyan law.

c. The Commission shall maintain a log of sites visited as a means of determining appropriate usage.

d. The Commission shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.
11.8 Email

(i) The Commission encourages the use of email and respects the privacy of users. The Commission will not routinely inspect, monitor or disclose the contents of email without the consent of the user. However, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the Commission may inspect, monitor, or disclose email when the Commission believes that it has a business need to do so. The use of email must be related to the Commission’s business activities.

(ii) For proper utilization of server disk space, uncollected mails will be disposed after every forty five (45) days. Mail users will be allocated disk quotas for storing mail. Use of email is permitted as long as it does not:

   a. Violate this policy
   b. Degrade the performance of the network and
   c. Divert attention from work

(iii) A disclaimer shall be applied to all outgoing email (See Annex i K)

12.0 PART VI- BUSINESS CONTINUITY POLICIES

Major operational disruptions pose a substantial risk to the continued operation of the Commission. The extent to which the Commission incorporates the risk of a major operational disruption in its business continuity plan is dependent upon its risk profile.

(i) The Commission shall ensure the implementation of the business continuity plan by periodically conducting a business impact analysis at least once a year.

(ii) An organizational risk assessment, risk management and risk monitoring to identify the mission critical activities and potential for major disruptions will also be undertaken. The Commission should also provide sufficient human and financial resources to support Business Continuity Management.

12.1 Responsibilities of the Commissioners and Top Management

The responsibility for business continuity management rests with the Commission and the senior management who are expected to formulate business continuity policy reviews, procedures and guidelines. All these must be documented and reviewed after every two (2) years.

Commissioners’ and senior management shall be responsible for:
(i) Institutionalising Business Continuity Management Document;
(ii) Defining the roles, responsibilities and authority to act in the event of a major disruption;
(iii) Constituting Business Continuity Management Team consisting of:
    a. Coordinator (drawn from the senior management);
    b. Department Heads;
    c. Line Managers; and
    d. Risk Management Officer.
(iv) Constituting Crisis Management Team consisting of all heads of critical operational areas;
(v) Accountability for business continuity management in cases of outsourced business continuity function.
12.2 Risk Assessment
A risk assessment examines the most urgent business functions identified during business impact analysis. It looks at the probability and impact of a variety of specific threats that could cause a business disruption.

The Commission shall undertake a Risk Assessment of its ICT processes every one (1) year.

12.3 Business Impact Analysis

Business impact analysis forms the foundation upon which the business continuity plan is developed. It identifies critical business functions and operations that need to be recovered on a priority basis and establishes appropriate recovery objectives for those operations. It should be completed in advance of a risk assessment in order to identify the urgent functions upon which a risk assessment should be focused.

12.4 Recovery

(i) The Commission shall develop recovery procedures that reflect the risk they represent to the operation of its systems taking into consideration the interdependency of risks.

(ii) The Commission shall facilitate testing of plans to ensure that crisis and recovery teams are aware of their roles and responsibilities in the event of a disruption.

(iii) In cases where the Commission shares or outsources a disaster recovery site, there must be service level agreements or contract in place that clearly outline the terms that govern these arrangements between the parties.

(iv) Recovery solutions must be based on Business Impact Assessment (BIA) information.
13.0 Monitoring And Evaluation

All ICT systems, as with all other assets, are the property of the Commission. The Commission therefore reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

(i) Users of the Commission’s ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the Commission’s ICT resources should avoid storing information on these systems that they consider private. By using the Commission’s ICT systems, users expressly consent to the monitoring of all their activities within the Commission’s ICT systems.

(ii) During the implementation of this policy, the Commission will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The Monitoring and Evaluation will be carried out by the ICT internal M&E team in consultation with the TSC M&E Technical Committee.

13.1 Compliance

All users of the Commission’s ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT. A sample declaration is provided in annex ii.

14.0 Policy Review

This policy will be regularly reviewed and amended as required to ensure it remains relevant and effective in meeting the Policy objectives. The responsibility for the ongoing review resides with the head of ICT in conjunction with the Commission ICT Governance Committee. Any proposals during intervening period should be submitted to the Head of ICT. Any changes to this policy shall be communicated to all users of the Commission’s ICT systems.
ANNEX I: POLICY IMPLEMENTATION GUIDELINES

A. Guidelines for Information Systems

1. Application Systems

   (i) The selection of a supplier or system developer should be carried out in accordance with the existing rules and regulations on public procurement.
   (ii) The duplication of copyrighted software or documentation is strictly prohibited unless for backup purposes.

2. Installation/operation

   The installation and operation of systems will involve the following:

   (i) Preparation of end users with awareness and training prior to deployment. [This is to ensure best results and to avoid unnecessary calls to user support].
   (ii) Maintenance of full documentation with respect to configurations, changes, and other “as installed” parameters. This will facilitate efficiency in management of operations, especially in the event of staff changes.
   (iii) Software will be installed in accordance with licence agreements.
   (iv) Software will be installed and rolled out only after issuance of an acceptance testing certificate.
   (v) Systems shall be commissioned only after being tested and accepted.

B. Guidelines on Operating Systems

   (i) Software drivers to support efficient use of the Microsoft Office suite will be accessible centrally from a designated server; and
   (ii) Updates of the Office Productivity software will be carried out as and when new versions are released.

C. Guidelines on antivirus software

   (i) Any new computer or laptop shall be installed with the most current antivirus software; and
   (ii) Any virus-infected computer must be removed from the system until it is certified as being virus free.

D. Guidelines for Personal Computers and Servers

   (i) Users are required to lodge a report of any malfunction of the computer they use on the prescribed problem reporting system or mechanism to the head of ICT;
   (ii) Laptops should not be carried out of TSC building except for Commission’s work outside the building. All laptops to be carried outside for external use must be logged;
(iii) Hardware specifications should be reviewed biannually by the head of ICT;
(iv) The operating environment for all data centres and server rooms should be consistent with the manufacturers’ specifications;
(v) Server storage should be structured logically and space allocation quotas enforced.

E. Guidelines for Procurement

(i) The head of ICT shall undertake an annual survey to determine needs and impact of ICT resources in the Commission;
(ii) Requests by any service area for the procurement of ICT related goods and services shall be validated by head of ICT;
(iii) Technical evaluation and inspection of ICT equipment shall be done under the supervision of the Head of ICT strictly on the basis of the technical specifications;
(iv) Deployment of procured ICT equipment shall be done by the Head of ICT, strictly on the basis of identified and validated needs;

F. Guidelines on operations

Guidelines covered under physical Security sub section shall apply.

G. Guidelines on inventory of ICT equipment

(i) Inventory must include serial number, date of issue, location/service area, model, type, head of service area, responsible officer and functional condition.
(ii) Inventory of computers should be reviewed and updated continuously.
(iii) The head of ICT shall conduct an annual inventory check of all ICT equipment.
(iv) In the event of any movement of ICT equipment from one office to another, the same should be communicated to the head of ICT for purposes of updating the inventory.
H. Guidelines for Decommissioning of ICT equipment
   (i) At the end of five (5) years after the procurement of the equipment, a review shall be done for the purpose of determining its continued usage, or discontinuity;
   (ii) For equipment that have been in existence for five (5) years and above, a comprehensive review shall be carried out immediately the policy is effective;
   (iii) For all newly acquired equipment, a post installation review shall be carried out 6 months after commissioning while subsequent reviews will be undertaken every two (2) years;
   (iv) All the data and software must be removed before decommissioning

I. Human Resources and Development Guidelines

The Commission will upgrade ICT skills and knowledge of all its employees and agents annually. This will include:

(i) End user training
   It is a requirement that all newly recruited TSC employees must possess basic computer skills.

   End user training programme will include the following content:
   a. Refresher course on basic computer user skills;
   b. Overview of ICT policies and guidelines;
   c. Skills specific to particular applications; and
   d. Security and best practices

(iii) Technical Training
   Technical training programme will include the following content:
   a. Support related training (depending on area of assignment and deployment);
   b. Professional Certification (in the area of specialization);
   c. Overview of ICT policies and guidelines;
   d. Security and best practices; and
   e. Advanced Data Communication and networks.

(iv) Management Training
   This level of training will programme will include the following content:
   a. Basic computer user skills;
   b. Overview of ICT policies and guidelines;
   c. Skills specific to particular applications
   d. Security and best practices;
   e. Use of management reporting tools.
J. System Controls and Security Guidelines

All users of the Commission’s ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the Deputy Secretary (ICT). A sample declaration is provided in the annex II.

Responsibilities

(i) The head of ICT has overall responsibility for security management policy. The officer shall:
   a. Ensure the compliance, establishment and implementation of the ICT security policy
   b. Provide support and guidance to assist users in understanding their responsibilities with regard to ICT security

(ii) Managers and supervisors are responsible for ICT security within their service areas. They should:
   a. Ensure that all users who report to them are aware of this policy and are in compliance with it
   b. Maintain appropriate control to ensure adherence to this policy
   c. Ensure that breaches of security are dealt with in a coordinated and timely manner and reported to the head of ICT.

(iii) Senior Deputy Secretary (Audit) will be responsible to:
   a. Ensure compliance with the Commission’s ICT security policy;
   b. Gauge the effectiveness of the ICT security measures through regular monitoring programs;
   c. Report to the head of ICT on the irregularities and any breaches of ICT security policy.

(iv) Systems Administrator

   Systems access rights will be granted by the system administrator.

(v) User Responsibilities

   The users of the Commission’s information systems are accountable and responsible for:
   a. Understanding and adhering to this policy; and
   b. Notifying any breach of ICT security to the head of ICT or immediate supervisor

(vi) Systems Access

   Access to ICT equipment and systems shall be restricted to authorized users through the use of logon identities, passwords, locks and access control devices. The use of system logon identities shall be unique to each authorized user. All logon identities shall be authorized by at least two managers of the respective system.

(vi) Physical Security

   The creation of user identities shall be as follows: -
a. Access to secure areas of the Commission shall be authorized by the Information systems security manager in consultation with the head of ICT;
b. Access to the Commission’s ICT network shall be authorized by the head of ICT; and
c. Access to the Commission’s business applications shall be authorized by the appropriate line manager

(vii) Physical Security Rules
The following rules relate to physical security:
   a. The Commission premises, and in particular secure areas, must be physically strong and protected against weather elements and hazards including rain, floods, fire, extreme temperatures, tremors, dust and lightning.
   b. Entry into secure areas will be restricted to unauthorized users;
   c. Visitors to secure areas shall be permitted only under strict supervision of an authorized ICT staff and a log shall be kept for each visit;
   d. Secure areas shall be protected against intrusion by use of appropriate surveillance systems or by security personnel;
   e. Combustible material shall not be kept near ICT equipment;
   f. Air temperature and humidity must be controlled within acceptable limits;
   g. All computer devices must be adequately protected against interruptions to electricity supply;
   h. Computing equipment must not be removed from the Commission’s premises unless written approval is given by the head of ICT or any other relevant authority.

(viii) The head of ICT must ensure that:
   a. Access to the server rooms is restricted to unauthorized users and that access is by an access control device;
   b. Server rooms are fitted with fire detectors and fire extinguishing equipment. The fire suppression equipment should preferably be set to automatically extinguish fire; and
   c. Air conditioning systems are functional in accordance with supplier standards.

(ix) Responsibilities of Information Security Officer
The officer must ensure that:
   a. Fire detection and prevention equipment are tested on a regular basis, at least twice a year
   b. Ensure that visitors to the Commission’s buildings have been authorized to gain access to the Commission’s premises.

(x) Responsibilities of TSC security personnel
Security must ensure that:
a. All ICT equipment leaving the TSC premises are accompanied by a valid authorisation by way of a gate pass;
b. There is consistency between the serial numbers on the equipment and the gate pass;
c. All non TSC ICT equipment coming into the TSC premises must be declared and registered

(xii) Responsibility of users

Users must:

a. Not remove any computer device from the Commission's premises without written approval by the head of ICT and Deputy Secretary (Office Services);

b. Safeguard their workstations against damage e.g. from dust, water etc

(xii) Passwords

All users with access to the Commissions ICT systems are responsible for taking appropriate steps in selecting and securing their passwords. Users should ensure that their passwords are periodically changed. It is essential that access to ICT systems should be through the use of strong passwords.

The following rules govern the use of passwords:

a. All passwords must be changed on at most a quarterly basis;
b. Passwords will consist of a minimum of 6 alphanumeric characters;
c. Passwords will be kept private i.e., not shared, or written down;
d. Logon IDs and passwords should be suspended after a specified period of disuse;
e. Logon IDs and passwords should be suspended after a set number of unsuccessful log on attempts;
f. Passwords should not be repeated or be similar to previous passwords, application systems will be set to remember the last 5 passwords;
g. Passwords should not be the word “password” or a similar word in English or vernacular;
h. Passwords should not be a common usage word such as:
   1. Names of family, pets, friends, co-workers etc;
   2. Computer terms and names;
   3. The words TSC or any derivation;
   4. Birthdays and other personal information such as addresses and phone numbers; and
   5. A word or number patterns like aabb, qwerty, zyxwvuts, 123321, etc.
   6. Employees will be formally notified as to their role in protecting the security of their user ID and password.
   7. Passwords stored on a computer should be encrypted in storage
   8. A non-printing, password-suppression feature should be used on all terminals to prevent the display of a user ID or password at log-on.
9. Procedures for forgotten passwords should require that the user be personally identified by Support Services.

(xiii) Data Security

a. In the event of confidential information being lost, either through loss of a computing device or other breach in security, the head of (ICT) should be notified immediately; No attempts should be made to recover data without authority from head of ICT.

b. Personal data such as music, video, images, documents should not be saved on the network server.

(xiv) Responsibilities of users

Users should:

a. Not use the same password for the Commission’s system accounts as for other non-Commission access (e.g., personal internet accounts etc.);

b. Where possible, not use the same password for various Commission systems needs. For example, users should select one password for Deputy Secretary (ICT) and a separate password for other ICT systems and a separate password to be used for an network account;

c. Never share passwords with anyone, including supervisors, system administrators, assistants or secretaries. If someone demands a password from them, users should refer the person to this document or to the EMIS - change to ICT division;

d. Never use the "Remember Password" feature of applications (e.g., Outlook, Messenger, Internet Explorer);

e. Never write passwords down or store them anywhere in the office, or on any computer system (including Palm Pilots or similar devices) without encryption;

f. Change passwords at least once every quarter;

g. Report to the Deputy Secretary (ICT) any suspected breach of password;

h. Log out or lock their workstation whenever they are away from the workstation for an extended period;

i. Avoid using previous passwords.

j. Any new password request should be done through a memo from the head of section to the head of ICT.

(xv) Responsibilities of Supervisors

Managers and supervisors should inform the Deputy Secretary (ICT) whenever a user is transferred or leaves the service of the Commission so that the user’s access rights can be withdrawn. Summary dismissals must be communicated to the Deputy Secretary (ICT) immediately.

(xvi) Responsibilities of the Deputy Secretary, (HR)

The Deputy Secretary (HR) must inform the Deputy Secretary (ICT) whenever a user is transferred or leaves the service of the Commission so that the user’s access rights can be withdrawn. Summary dismissals must be communicated to the Deputy Secretary (ICT) immediately.

(xvii) Responsibilities of Head of ICT

The Head of ICT must ensure that:
(a) A backup policy and procedure that covers all Commission data is developed;
(b) The necessary storage space for users to store important Commission information is provided; and
(c) Backups of Commission data are stored in an access-controlled area.
(d) Database integrity is achieved

(xviii) Responsibilities of Users
Users must ensure that:
  a. All Commission data and files are saved on a network server for which they have been assigned as opposed to the local hard disc;
  b. Portable computer storage devices must be stored securely when they are not being used; and
  c. Portable computer storage devices that are to be disposed off must be done so securely.

(xix) Copyright and license agreements
All software used on the Commission’s ICT system must be licensed;

(xx) Responsibilities of Deputy Secretary (ICT)
The Deputy Secretary (ICT) must ensure that only authorized software is installed on the Commission’s ICT systems

(xxi) Responsibilities of Users
Users must not:
  (a) Install any software on their PCs without the knowledge of the Deputy Secretary (ICT);
  (b) Copy, distribute or remove software without the written authority of the Deputy Secretary (ICT);
  (c) Download and install any software from the internet without the written authority of the Deputy Secretary (ICT)
  (d) Should not know the administrators password of their PC

(xxii) Computer Viruses
The following rules govern the use of the anti-virus application:
  a. All virus definitions must be current and should not be more than two weeks old
  b. Any PC on the network should be scanning for viruses automatically as it boots

(xxiii) Responsibilities of Deputy Secretary (ICT)
The Deputy Secretary (ICT) ensures that:
  a. Anti-virus systems are kept current. Daily administration of the anti-virus application is planned and automatic updates to definitions are made.
  b. Apply any updates to the services it provides that are required to defend against threats from viruses.

(xxiv) Responsibilities of users
Users must ensure that:
  a. Their workstations are running an anti-virus application
b. They should not disable or remove anti-virus applications or the automatic update feature

c. They should treat any unexpected email attachment suspiciously and delete the email if unsure of the origin

d. They do not write, distribute or introduce any software known or suspected to be infected with a virus to the Commission’s ICT systems

(xxv) The following rules govern the use of the Commission’s Internet access:

(a) Use of the Internet is permitted as long as it does not violate this policy and does not degrade the performance of the network and divert attention from work.

(b) Use the Internet to Solicit, Reveal or publicise TSC confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

(c) Damage, alter, or degrade equipment providing internet and network connections thus, hindering others in their use of the Internet.

(d) The Commission will seek to interlink all its offices through extranets and use of remote access technologies, with selective access granted to teachers, suppliers, customers, or other partners.

(e) The Commission shall maintain a presence on the Internet and promote interactivity with its clients through its corporate portal.

(xxvi) Users shall not:

(a) Download or store music, media or any other files where copyright issues may be of concern;

(b) Use the Commission’s Internet facility for running private businesses;

(c) Upload, download, or transmit:
   1. Copyrighted materials belonging to third parties
   2. Offensive, fraudulent, threatening or harassing materials

(d) Propagate computer viruses, run peer-to-peer software, send and/or receive unofficial files or undertake activities that cause network congestion;

(e) Gain unauthorized access to any computing, information, or communications devices or resources

K. Email Guidelines

(i) The following disclaimer will be applied to all outgoing email:

“This email is confidential and intended for the sole use of the individual or entity to which it was addressed. If you have received this email in error please notify the sender immediately and delete this email without disclosing copying using distributing or storing its contents. Kindly note that unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Commission. The recipient should check this email and any attachments for
the presence of viruses. Commission accepts no liability for any damage caused by this
email.”

(ii) Email must not be used to:
   a. Reveal or publicize confidential or proprietary Commission information
   b. Send or forward emails containing defamatory, ethnic, offensive racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
   c. Send copies of documents in violation of copyright laws
   d. Harass, intimidate or interfere with the ability of others to conduct the Commission’s business.
   e. “Spoof” i.e. sending an email so as it appears to be from someone else.
   f. “Snoop” i.e. obtaining access to the email of other people for the purpose of satisfying ones morbid curiosity
   g. Attempt to breach any security measures on the email system
   h. Attempt to intercept any email transmission without proper authority
   i. Send “Spam” i.e. unsolicited email messages
   j. Propagate viruses or generate high volume of network traffic that degrades the performance of the network
   k. Send confidential emails without the use of suitable encryption.

L. Business continuity
   (i) Office, data centre or server room recovery must not be in the same building or close to the normal business operation.
   (ii) Documented pre and post test reports are to be completed for all recovery testing.
M. Risk Assessment

(i) The BC Management Team shall report on the status of business continuity management to the Commission and senior management on a regular basis, highlighting where there are identified gaps. This is through implementation status reports, incident reports, testing results and related plans for strengthening the business continuity plan.

(ii) A risk assessment is at a minimum expected to achieve the following:
   a. Identify unacceptable concentrations of risk and what are known as ‘single points of failure’.
   b. Identify internal and external threats that could cause a disruption and assess their probability and impact.
   c. Prioritize threats within the institution.
   d. Provide information for a risk control management strategy and an action plan for risks to be addressed.
   e. Mitigation of risks through a documented remedial plan.

(iii) Methods and Techniques
   The methods and techniques to be used to provide risk assessment include;
   a. Insurance statistics;
   b. Published disaster frequency statistics;
   c. Scoring systems for impact and probability;
   d. Gap analysis; and
   e. Stress testing.

N. Business Impact Analysis (BIA)

At a minimum a business impact analysis is expected to;

(i) Provide an understanding of TSC’s most critical objectives, the priority, and the timeframes for resumption of each;

(ii) Provide information about resource requirements over time to enable each business function within the organization achieve continuity or resumption of activity within the established timeframes. It should at a minimum identify:
   a. Staff numbers and key skills;
   b. Data applications and systems;
   c. Facilities including alternative location needs, backup strategy policy and schedule. Vendors/ suppliers of various services;
   d. Constraints;
   e. Mission Critical Activities (MCA’s) or tasks that need to be recorded to ensure continuity of the process and business;
   f. Dependencies on people, systems, processes, internal and external parties;
   g. Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) for every MCA or business;
   h. Systems impact assessment highlighting;
   i. Location;
(iii) Methods and techniques

A combination of the following tools and techniques may be used to carry out Business Impact Analysis:

a. Questionnaires.
b. Interviews.
c. Workshops.

(iv) Generally a combination of all the above methods should provide an adequate source of information from which to base the Business Continuity Plan. All relevant information should be stored for reference for at least one year or until the next BIA.

(v) Business Impact Analysis (BIA's) must be signed off by department or functional heads through a formal functional process stipulating that they understand, accept and verify BIA’s are correct.

P. Recovery procedures

(i) The business continuity plan should address staff requirements and relocation to the alternate site in the event of a major disruption. A detailed list of tasks for offsite recovery should be made available to all concerned staff.

(ii) TSC business continuity management team should:

a. Identify those business functions and operations to be recovered on a priority basis and establish recovery procedures.
b. Establish recovery procedures proportional to the risk they pose to the financial system.
c. There are measures for the quality of planning, competency of staff and effectiveness of the business continuity plan.
d. There is organizational awareness of emergency procedures and team members and staffs are familiar with their roles, accountability, responsibilities and authority in response to an incident.
e. All technological, logistical and administration aspects of the business continuity plan have been tested.
f. The recovery of infrastructure including command centers and off site work area is assured.
g. The availability and relocation of staff is assessed.
h. Documentation of testing results for the Commissioners, senior management, and auditors.
i. An inventory of assets needed for offsite recovery should be generated.
j. The alternate site should be sufficiently equipped with the necessary equipment, data and to maintain critical operations and services for a sufficient time period.

(iii) Methods and techniques
Management should develop a test plan for each BCP testing method used. TSC should employ various methods of exercising including but not limited to the following:

a. Technical tests.
b. Desktop / Orientation/ walkthroughs.
c. Live runs.
d. Simulations.
e. Integrated tests for departments that are dependent on each other and also stress testing of recovery facilities.

(iv) Communication
TSC should include in its business continuity plans procedures for communicating within the Commission and with relevant external parties in the event of major disruptions. The Commission shall ensure that the response to a disruption is communicated internally and externally to applicable parties. External communication to the media must only be through the external communications teams and approved by senior management or the Commission.

(v) The communication procedures should:

a. Ensure that there is a clear plan identifying staff, for communicating internally (within the organization) and externally (to the public) stakeholders.
b. Establish communication protocols clearly outlining the chain of command from the Commission, Commission Secretary, and Senior Management;
c. Develop a directory for all recovery team members including the crisis management and emergency management teams, local emergency response organizations and critical service providers.
d. Ensure that the directory/contact lists are made available to all team members.
e. Address obstacles that may arise due to failure in primary communications systems (electricity, mobile phone network, road network). Ensure that the institution has set up alternative modes of communication.
f. Ensure that copies of business continuity plans are disseminated to the relevant personnel.
ANNEX II: ACKNOWLEDGEMENT OF ICT SECURITY POLICY

I have read and understood the Commission’s ICT security policy. I will adhere to the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

ACCEPTANCE

Name: _______________________________________________________

TSC Number:---------------------------------------------

Signature: ____________________________________________________

Date: ______________________________________________
ANNEX III: ICT GOVERNANCE COMMITTEE STRUCTURE

COMMISSION SECRETARY
(CHAIRMAN)

SDS (ADMIN)  SDS (F)  SDS (S)  SDS (IA)  SDS (HR)  HEAD - (ICT) SECRETARY