TANZANIA BUREAU OF STANDARDS

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) POLICY

NOVEMBER, 2017

PREFACE

This TBS Information and Communication Technologies (ICT) Policy is a set of commitments and principles intended to govern the development, adoption and application of ICT at the Bureau. It provides the rationale and philosophy to guide the planning, development and utilization of ICT as a vehicle towards the realization of the Bureau's strategic goals and objectives.

The Policy articulates issues and statements and sets out guidelines to be adhered to in all decisions concerning ICT in order to maximize effective use of ICT for enhanced efficiency in service delivery. It sets standards for acceptable use of TBS ICT resources, security standards for safeguarding ICT resources, and provides direction as to how ICT should be used to enable and enhance the delivery of TBS services by improving efficiency and effectiveness.

The Policy sets a framework that should effectively support successful deployment, utilization and mainstreaming of ICT in all functions of the Bureau, to drive the implementation of the Bureau's corporate goals and objectives. It sets a basis for the Bureau's commitment in various areas including ICT leadership and governance, software and hardware management, service business continuity and disaster, ICT security, internet use and confidentiality. Further, it sets out guidelines on prohibited conduct, ICT acceptable use, security issues, defines responsibilities, recommends implementation modalities and outlines the Bureau's commitment in ensuring the availability of ICT expertise, hardware and software.

Various reasons necessitated the review of the TBS ICT Policy of 2010. First and foremost, the Policy was due for routine review and it was important to review it to ensure that it still meets the objectives of the organization in ICT matters. However, various other reasons necessitated the review of the policy, including fast changes in technology which require planning in order to avoid the issues of incompatibility and inaccessibility, gaps in ICT expertise, the growth of the Bureau in terms of employees, services and customers, and the need to be in line with the National ICT Policy, e-Government Strategy and Policy and other relevant government initiatives.

This Policy is tailored to suit the current situation at the Bureau. It was prepared in accordance with the National ICT Policy 2003 and in line with the Tanzania Development Vision 2025, the National Strategy for Growth and Reduction of Poverty (NSGRP) and the Sustainable Development Goals (SDGs). It will serve as a guide for Management in strategic planning and deployment of ICT.

The Policy will be used alongside other relevant policies, regulations, directives and national laws on matters relating to ICT. It is subject to review/amendment every after five years and when need arises to align it with the prevailing environment.

When this Policy is in conflict with the National ICT Policy or any such other national policies, laws, regulations and directives, the National ICT Policy and such other national policies, laws, regulations and directives shall prevail.

Dar es Salaam
November, 2017

Eng. Tumaini Mtitu
Acting Director General
Tanzania Bureau of Standards

LIST OF ACRONYMS

AOL – American Online
CD – Compact Disc
CD ROM – Compact Disc Read Only Memory
ICT – Information and Communication Technologies
ICT SC – Steering Committee
ID – Identification
SDGs – Sustainable Development Goals
NSGRP –National Strategy for Growth and Reduction of Poverty
PC – Personal Computer
QUALIMIS – Quality Management Information System
R&D – Research and Development
TANCIS – Tanzania Customs Integrated System
TBS – Tanzania Bureau of Standards
TRA – Tanzania Revenue Authority
TRAPAD – TRA-Pre-Arrival Declaration
USB – Universal Synchronous Bus

DEFINITION OF TERMS

For the purpose of this Policy, the following definitions shall apply;

"Computer virus" is a malicious computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus can also transmit itself across a network, spreading the infection to other computers and devices.

"**Management**" is as defined in the Standards Act No. 2 of 2009 as amended from time to time.

"Policy" means the Tanzania Bureau of Standards Information and Communication Technologies (ICT) Policy.

"Security breach" is an activity which causes or has the potential to cause the loss, damage or corruption of data.

"Security incident" is a situation where the security of a PC, a system, an application or the network has been compromised, and may be from an internal or external source.

"Security violation" is any activity which contravenes the ICT security and other related policies, procedures and guidelines and may result in a security breach.

"Security weakness" is a situation whereby a potential for a security incident is identified.

1.0 INTRODUCTION

1.1 Background

The world's advances in ICTs over the past 20 years have been phenomenal. A candid examination of our daily and office lives illustrates ICTs' impact on how we communicate, work and learn. As a result, the digital age has brought about remarkable transitions in office operations. Consequently, most workplaces today acknowledge ICTs' pivotal role in daily operations as ICT use enhances effectiveness, efficiency, transparency and productivity.

These rapid technological advances have brought rapid changes in knowledge management, covering aspects of knowledge creation, processing, storage, sharing, dissemination, collaboration and human resource development, in the level of education and training as well as work output and productivity. To overcome the lag in adoption of ICT, Tanzania Bureau of Standards (TBS) Management has committed to the development of an Information and Communication Technology (ICT) Policy that will build on existing corporate initiatives and support in achieving the Bureau's mission. As a consequence of pursuing its mission, it is anticipated that the Bureau will benefit from investing in ICT.

This Tanzania Bureau of Standards (TBS) Information and Communication Technologies (ICT) Policy lays down the framework for ICT development at the Bureau and provides guidance on the acquisition, use, maintenance and disposal of ICT hardware and software. The Policy is comprised of statements showing Management commitment in development of an ICT infrastructure capable of leading the Bureau towards its desired direction. It is intended to guide the development of procedures for Management and staff practice in ICT matters.

1.2 Institutional overview

In general, most TBS employees have computers and/or internet access. In many offices computers are not shared. In offices where computers are shared they are shared by at most 2-3 people. At the time of this analysis, TBS had more than 200 desktop computers, 30 laptops, two (2) rack mountable and three (3) medium tower servers, six (6) Cisco switches, nine (9) D-Link switches and 57 printers.

Most staff members have basic knowledge in microcomputer applications such as Microsoft word and excel. The Bureau also has a website which administered and maintained by TBS staff. The maintenance of ICT equipment is carried out by ICT technician and in the absence of internal capacity maintenance is outsourced.

Since the introduction of ICT Section at TBS in 2008, various initiatives have been taken to integrate ICT in standardization, quality assurance and support activities. Currently, the Bureau runs various management information systems which are used in performing various activities. The systems include the Quality Management Information System (QUALIMIS), Peak-Payroll, Microsoft Business Solution (Navision), Daily register system (Biostar) and others. The Bureau is also linked to various other nationwide systems such as Tanzania Customs Integrated System (TANCIS), TRA-Pre-Arrival Declaration (TRAPAD) system and Human Capital Management Information System (Lawson). The Bureau is currently working on a system that will enable online sale of standards (webstore).

This cursory review of the ICT status at TBS indicates that there are significant developments taking place. Nonetheless, more efforts are needed in terms of resources and capacity building.

Meanwhile, a concerted effort is required to address existing gaps and ensure a positive impact of ICT integration in standardization and quality assurance activities.

1.3 Rationale

Major reasons for formulating this ICT policy include but are not limited to the following:

a) Rapid changes in technology. In relation to changes in technology, generally planning becomes increasingly important in order to avoid issues of incompatibility and inaccessibility. It is a known fact that ICT technology changes very fast in the world and as such there is a need for having in place a policy framework for developing and maintaining institution-wide ICT systems.

b) Inadequate ICT expertise. The big gap of adequately trained and experienced human resources constrains ICT developments and therefore requires that priorities be established within an ICT policy.

c) Inadequate human, material and financial resources. Constraints in human, material and financial resources are a major reason for high level ICT planning which among other requires sound policies.

d) General growth. The development of products, services, research, technological activities, policies and methods as well as the growth of the number of customers will depend on the availability of ICT services and systems. It is equally important to understand this dependency at an early stage which is very critical in order to achieve the success of an ICT policy implementation.

e) Integration of TBS activities with national initiatives. In line with the National ICT Policy, e-Government policy and other government initiatives, TBS needs to develop an institutional policy that will guide the governance and implementation of ICT infrastructure.

1.4 Policy scope

This Policy covers all ICT and ICT-related activities, users and resources including computers, computer systems, applications, networks, software, media and files.

This policy will also guide acquisition further development, administration, maintenance and usage of the ICT facilities. With adequate investments in ICT, this policy document can be implemented to the advantage of the internal and external TBS customers.

2.0 POLICY CONTEXT

This Policy is built on an assumption that in the modern world, ICT is a part and parcel of an organization and an indispensable component in determining the strategic direction of the organization. The Policy originates from a number of policy documents as identified below:

a) The Tanzania Development Vision 2025
b) The National Strategy for Growth and Reduction of Poverty (NSGRP)
c) The Sustainable Development Goals (SDGs)

d) National Information and Communications Technologies Policy

e) Other Related National ICT Initiatives:

Tanzania is in the process of implementing a number of policies, strategies and initiatives that will all impact the integration of ICT into public service. Some are directly related to national ICT infrastructure and include the National ICT Backbone Infrastructure initiative, implementing the National e-Government Strategy, and the Rural Telecommunications ICT Fund. It is imperative that the implementation of this Policy takes cognizance of current and emerging programmes of this nature with a view to reducing costs, not duplicating efforts and increasing value through synergies.

3.0 ICT MISSION AND VISION

3.1 Vision

To be a strategic guidance to the Bureau's ICT resources towards becoming a proficient institution in standardization, quality assurance and metrology services.

3.2 Mission

To ensure proper use of ICT resources in promoting standardization and quality assurance services through improved ICT infrastructure, business operations and well-trained staff.

4.0 POLICY OBJECTIVES

4.1 General Objectives

This ICT Policy has the following General objective:

To support the strategic vision of TBS by improving operational efficiency and exchange of information through the appropriate application of ICT in standardization and quality assurance activities.

4.2 Specific Objectives

This TBS ICT Policy aims to achieve the following specific objectives:

a) Set standards for acceptable use of TBS ICT resources.

b) Set security standards for safeguarding ICT resources covering computer systems, applications, networks, software, files, etc.

c) Providing direction as to how ICT will be used to enable and enhance the delivery of TBS services by improvement of efficiency and effectiveness of its activities.

d) Provide a clear ICT framework for every member of TBS staff and key stakeholders.

e) Enhance the corporate level of awareness as to the role and potential of ICT, with emphasis on sustainable development, in the empowerment of people and in enhancing governance.

f) Accelerate innovation to develop a knowledge based system.

g) Increase the competitiveness of national industry with the establishment of an adequate ICT based standardization infrastructure.

h) Improve the access of clients to standardization and quality assurance services.

i) Provide the availability of ICT access points in all areas and implement a cost-effective
j) ICT.

k) Reduce operational costs and improve the quality services through the application of ICT.

l) Promote the development of ICT-literate human resources necessary for driving the standardization and quality assurance agenda.

m) Enforce the awareness of the role ICT plays within the context of standardization and quality assurance.

n) Promoting information sharing, transparency and accountability and reduced bureaucracy in operations.

o) Identify priority areas for ICT development in terms of innovation, research and development.

5.0 POLICY STATEMENTS

The Tanzania Bureau of Standards (TBS) ICT Policy statements have been categorized into the following 22 areas:

5.1 ICT Management, Leadership and Governance

5.1.1 ICT leadership

Policy Statements

TBS shall

i) ensure that, ICT Steering Committee is in place to foresee the IT Governance activities including the main role of providing leadership and aligning all ICT investments, decisions and initiatives with overall TBS's business objectives.

ii) have an effective institutional arrangement for establishment of the ICT section/department.

iii) ensure ownership of the ICT Policy and ICT Strategy through ICT Steering Committee (ICT SC).

5.1.2 Corporate obligation

Policy Statements

TBS shall

i) provide the network, personal computers, electronic mail and other communication devices for staff use to support its functions of standardization and quality assurance including supporting activities.

ii) provide a reliable network operating at the fastest speed. Such a network shall be economically viable and capable of providing staff with inter-connectivity to both national and international networks.

iii) build a solid foundation of ICT infrastructure and shall establish a sound fiscal planning that shall guarantee the state-of-the-art maintenance of the infrastructure.

iv) provide adequate resources for regular maintenance of the ICT equipment (computers, servers, etc.).

v) ensure that its employees are informed of the type of behavior it expects from them in the use of ICT at the workplace and about the consequences for abusing the technologies.

5.2 ICT Procurement

Policy Statements

TBS shall

i) develop and implement procurement plan and procedural guidelines to properly guide staff on procurement procedures for timely procurement of ICT systems and facilities.

ii) implement procurement procedures in accordance with the Public Procurement Act in relation to annual procurement plan.

iii) procure ICT systems based on standards approved by ICT Steering Committee.

iv) ensure that procurement of ICT hardware and software is coordinated by the ICT Department. This ensures that equipment in use across TBS is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

5.3 Outsourced ICT Services

Policy Statements

TBS shall

i) define the outsourced services and maintain an inventory list of reputable vendors, suppliers and consultants.

ii) only outsource ICT services in the case where the ICT staff skills and opportunities are not sufficient to build capacity within TBS. Alternatively, TBS shall do so to relieve staff to concentrate and focus on their core business activities within the organization.

5.4 ICT Software and Hardware Management

5.4.1 Installation, distribution and safety

Policy Statements

TBS shall

i) ensure that software are installed, used and complied with the licensing management best practices.

ii) ensure that only legally licensed software are installed in TBS computers.

iii) ensure that correct licensing arrangements are followed when installing software.

iv) ensure the software are licensed according to the business needs through approved appropriate software assessment procedure.

v) distribute ICT hardware and software based on the approved business needs assessment. The business needs assessment shall be reviewed on annual basis.

vi) ensure that movement of hardware get approval of Management through consultations with the supervisor of the business area as per hardware movement guidelines.

vii) ensure that ICT hardware are safe and in case of loss or damage by negligence, the staff entrusted with the hardware shall be held liable. All the hardware will remain property of TBS.

viii) ensure that appropriate action is taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.

ix) discourage modifications to existing software and ensure that when modifications are necessary, they shall be authorized by Management and be processed as per appropriate procedures.

5.4.2 Software usage

Policy Statements

TBS shall

i) ensure that its employees use the standard software provided by the Bureau. Staff members shall not download applications, demos or upgrades without Management's authority.

ii) ensure that employees use the standard e-mail system provided by TBS for official e-mail communications, and shall not install their own e-mail systems.

5.5 ICT Service Business Continuity and Disaster

Policy Statements

TBS shall

i) develop and implement a feasible disaster recovery plan.

ii) ensure that the disaster recovery is reviewed regularly in accordance with new risks in order to maintain ICT services business continuity.

iii) ensure that sufficient resources are provided for effective implementation of disaster recovery plan.

iv) ensure that backup is exercised on regular basis on all systems software, application software, data and documentation to enable recovery with minimum business disruption and data loss.

5.6 ICT Service Management

Policy Statements

TBS shall

i) ensure ICT service management is implemented based on the best practice standards and approved business processes that shall be reviewed on demand.

ii) ensure ICT service management is implemented based on the approved ISO standards with clear key performance indicators as per business objectives.

5.7 ICT Service Provision

Policy Statements

TBS shall

i) outsource ICT services only to trustworthy service providers.

ii) improve government services through the application of ICT.

iii) ensure that for every outsourced service, there is a linkage with Service Level Agreement based on appropriate penalty measures (clauses).

iv) ensure that all service providers/vendors comply with Service Level Agreements.

5.8 ICT Security

5.8.1 Network security

Policy Statements

TBS shall

i) monitor network security on a regular basis.

ii) lodge adequate information concerning network traffic and activity to ensure that breaches in network security is easily detected.

iii) implement and maintain procedures to provide adequate protection from intrusion into its computer systems from external sources.

iv) ensure that no computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network.

v) ensure that its staff do not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

5.8.2 Network access

Policy Statements

TBS shall

i) ensure that access to its network, equipment, application, database or other ICT resources is by individual login – i.e. unique user name and password.

ii) ensure that all non-TBS computing equipment are only used to access TBS network resources if authorized by Management.

iii) ensure that each individual who is authorized to access TBS network is given a profile which limits his or her access to approved data, files and software.

5.8.3 Access to systems and applications

Policy Statements

TBS shall

i) ensure that access to systems and applications is restricted according to the role and business requirements of each user.

ii) ensure that a segregation of duties is implemented within a system or application to prevent accidental or deliberate misuse of the system or application.

iii) ensure that duties or responsibilities which may give rise to a conflict of interest if carried out by the same individual in a system or application are separated.

iv) ensure that access rights comprising the functions of read, write, delete and execute are allocated to each user in respect of each system and application.

v) ensure that established access rights are reviewed at an agreed interval to ensure that access to systems and applications remains appropriate and consistent. A review shall also take place after any changes to the system, such as an upgrade.

vi) ensure that access by the Systems Administrator is kept to a minimum number of individuals required to enable day-to-day operation and emergency access in the event of a system failure. Systems Administration access shall be via unique individual ID.

vii) ensure that privileges in systems and applications are allocated in a restricted and controlled manner.

viii) ensure that system and application privileges are removed when no longer required.

ix) ensure that access to systems and applications by third parties, such as partner organizations or contractor or software maintenance/support personnel is subjected to authorization and compliance with the TBS ICT security element.

x) ensure that access to systems and applications by third parties is restricted to only those systems, or parts of those systems, that are required and shall be revoked as soon as it is no longer required.

5.8.4 Physical security

Policy Statements

TBS shall

i) ensure that all hardware devices bear an identification number, which shall not be removed throughout the life of the device.

ii) ensure that all desktop devices, e.g. PC, printer and scanner, have adequate precautions taken to protect them against theft and accidental damage in addition to

environmental threats and hazards. It shall ensure that all manufacturers' and suppliers' instructions and advice are followed.

iii) ensure that all computers and equipment are turned off when not being used for an extended period of time.

iv) ensure that all ICT equipment are protected centrally by an Uninterruptible Power Supply (UPS) and where necessary controls shall be in place to ensure a clean power supply by eliminating the impact of power spikes.

v) ensure that all portable devices such as laptop computers are retained in a secure environment when not in use. This may include a lockable store cupboard with controlled access.

vi) ensure that all portable devices are security marked as soon as they are received and then added to the appropriate inventory. The same shall be traceable.

vii) ensure that users take adequate precautions to protect portable devices against theft or accidental damage at all times when they are taken off premises, e.g. by not leaving them visible but locked away.

viii) ensure that records are maintained within each department detailing their portable devices including type, serial number and software available, including the provision for signing out and return.

ix) ensure that all computer consumables (disks, etc) are retained in a secure environment wherever possible and issued only for TBS activities.

x) ensure that ICT consumables are not used for private purposes.

xi) ensure that server rooms, data centres and all other secure or sensitive areas are subject to additional security measures including controlled and authenticated access.

5.8.5 PC security

Policy Statements

TBS shall

i) ensure that all PCs are configured with virus protection software, which shall not be removed or disabled by users.

ii) ensure that each employee is responsible for protecting his/her computer against virus attack by following ICT guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on his/her workstation.

iii) ensure that all data disks and files entering or leaving TBS are scanned for viruses.

iv) ensure that staff log out of the network and turn their computers off before leaving the office or when away from their desks for an extended period of time.

v) ensure that a computer shared by a number of users is logged off by all users before it is left.

vi) ensure that a computer user is responsible for all work carried out on a computer using their login details, including internet access and e-mail use, whether or not that user was actually using the computer himself/herself.

5.8.6 Information and network infrastructure security

Policy Statements

TBS shall

i) adequately secure and protect its information resources including systems and data from unauthorised users or malicious attack.

ii) ensure that the three principles of information security (Information Confidentiality, Information Availability and Information Integrity) are not compromised.

iii) protect its network infrastructure from attacks using appropriate tools such as firewalls, intrusion detection systems and other means.

iv) ensure that information security awareness programmes are periodically conducted to members of staff and other stakeholders.

v) ensure that all members of staff comply with the Information Security Policy standards, procedures and guidelines.

vi) ensure that infrastructure and networks are robust and resilient and have adequate security, redundancy and backup arrangements.

vii) ensure that e-mail messages are treated as confidential and accessed only by the intended recipients.

viii) ensure that employees do not retrieve or read any e-mail messages that are not sent to them.

ix) ensure that employees do not use passwords, access a file, or retrieve any stored information unless authorized to do so.

x) ensure that security incidents, weaknesses, breaches and violations are reported as soon as possible to the ICT Department.

5.8.7 Passwords

Policy Statements

TBS shall

i) ensure that all passwords to ICT systems, databases and equipment are assigned by an appropriate authority.

ii) ensure that passwords to ICT systems, databases and equipment are not given to other staff or persons outside TBS.

iii) ensure that passwords to ICT systems, databases and equipment are not stored in computer data files, on the network, or are displayed openly at any workstation.

5.9 Message Content

Policy Statements

TBS shall

i) ensure that the Bureau's e-mail system is not used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.

ii) ensure that its e-mail system is not used to create any offensive or disruptive messages. Offensive messages include those which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

iii) ensure that any data or information on the system is not be deemed personal or private by its employees. In this regard, the e-mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

5.10 Storage and Backup

Policy Statements

TBS shall

i) ensure that all network data and file resources are backed up regularly.

ii) ensure that all backup devises and media are supplied by the ICT Department and that employees are not using personal backups for official data.

iii) ensure that all computer users back up their data as per the appropriate backup procedure.

iv) ensure that data is not stored or backed up on a computer's hard drive as it may be accessible to anyone switching on the PC. A computer hard drive is not secure and shall therefore be seen as a temporary, short term solution.

v) ensure that no data is stored on non-TBS equipment.

5.11 Access to Computers

Policy Statements

TBS shall

i) provide computer user accounts to all its staff. External people who are determined to be strategically important to TBS, such as temporary staff, volunteers, or contractors, shall also be provided user accounts as appropriate, on a case-by-case basis which shall be determined by the TBS Management.

ii) ensure that employees managing temporary or contract staff is responsible for the identification of access requirements and use of computer user account.

iii) revoke a computer user account when the employee terminates employment with TBS.

5.12 Internet Use

Policy Statements

TBS shall

i) ensure that its internet is used for standardization, quality assurance and supporting activities only.

ii) ensure that employees with internet access do not access, view, download, or print pornographic or other sexually explicit materials.

iii) ensure that employees are aware that there is no assurance that e-mail texts and attachments sent within TBS and on the internet shall not be seen, accessed or intercepted by unauthorized parties.

5.13 Virus Prevention and Control

Policy Statements

TBS shall

i) use a single anti-virus product for anti-virus protection. The software to be used shall be approved by Management.

ii) ensure that the approved anti-virus is deployed on a server and installed remotely on client computers.

iii) ensure that the anti-virus is set to scan automatically all client computers and servers once per day and that anti-virus library definitions are updated at least once per day.

iv) ensure that all software are checked for viruses before installation on any TBS device, including computers, laptops and other portable devices.

v) ensure that CD ROMs, USB memory sticks or other storage media is checked for viruses checked before use, when used to transfer files, program or data, from one machine to another, particularly if it is from an external source, a different department or service or from a standalone machine which may not be fully protected against viruses.

vi) ensure that all files downloaded from the internet are initially saved onto the user's hard drive (C: drive) and virus checked before opening or executing. Only when it has been found to be clear of viruses can it then be transferred safely to other areas, such as shared folders.

vii) put a mechanism in place to ensure that if a virus is found, or suspected to be on a machine or external storage media, the ICT Department is informed immediately.

viii) ensure that users are always notified through e-mail or any other means, concerning a particular virus and its effect and all users shall take appropriate action when so notified.

5.14 Confidentiality

Policy Statements

TBS shall

i) ensure that its employees safeguard the security of confidential and/or personal data for which they are responsible, or which they access in order to carry out their activities and also bring to the supervisors' attention any areas of concern regarding the transfer or transportation of such information.

ii) ensure that personal and sensitive corporate data is not disclosed, transferred, or copied to third parties without authorization from an appropriate authority.

iii) ensure that e-mail is not used for sending sensitive corporate data as its security cannot be guaranteed.

5.15 Disposal of Media and Equipment

Policy Statements

TBS shall

i) ensure that PCs which have become obsolete or are surplus to requirement have their hard disks checked for content.

ii) ensure that software that is being transferred to another machine is uninstalled and all data files are deleted.

iii) ensure that data storage devices are purged of sensitive data before disposal or securely destroyed.

5.16 Enterprise Architecture

Policy Statements

TBS shall

i) ensure its enterprise architecture align with National Enterprise Architecture.

ii) ensure its staff are adequately and constantly trained on Enterprise Architecture design, implementation and maintenance.

iii) implement a common Enterprise Architecture based on international standards on which all the ICT systems and business systems will be implemented.

iv) determine the Information, Applications and Technical systems architecture. These standards shall be determined through the ICT Steering Committee.

5.17 ICT Standards and Quality Control Practices

Policy Statements

TBS shall

i) ensure quality assurance, control and standards and uniformity of ICT resources across the organization are maintained.

ii) ensure that it acquires systems that can be integrated in a standard platform in order to achieve organization objectives.

iii) adopt an open source over proprietary technology for deployment of its ICT products when necessary and appropriate.

5.18 Software Migration, Upgrading and Change Management

Policy Statements

TBS shall

i) deploy new release of software upon approval through quality assurance and software testing procedure.

ii) implement change management procedure for infrastructure, software migration and upgrades.

iii) ensure prompt upgrades of software systems and availability of reliable technical support.

5.19 Monitoring and Evaluation

Policy Statements

TBS shall

i) develop and maintain monitoring and evaluation approaches to safeguard efficient and effective implementation of ICT policy.

ii) implement monitoring and evaluation system in order to measure success of implementation of all ICT projects.

5.20 Compliance to Relevant, Policies and Legal Requirements

Policy Statements

TBS shall

i) comply with all government relevant policy guidelines, laws and regulations related to its business.

ii) ensure that it conducts its business according to applicable laws.

iii) ensure its ICT Policy complies with the National ICT Policy, e-Government Policy and any other relevant government policies, laws and regulations for appropriate business execution.

5.21 Innovation, Research and Development

Policy Statements

TBS shall

i) adopt a state-of-the-art technology where there are optimal business benefits and availability of adequate technical support.

ii) conduct research, develop and establish procedures for adopting new technology.

iii) encourage Innovation, Research and Development (R&D) in the organization.

5.22 Human Resources and Training

Policy Statements

TBS shall

i) ensure that appropriate schemes of service are established, that are attractive to recruit and retain competent and experienced staff.

ii) ensure that all end-user staff undergo ICT training and awareness and acquire appropriate skills to enable them fully utilize ICT resources in the organization.

iii) ensure that all ICT technical and support staff undergo appropriate training to march with technological change requirements to enable them develop necessary skills and competencies.

iv) allocate funds in each annual budget for supporting ICT training.

v) ensure that capacity for research & development in IT is enhanced and innovation is encouraged.

vi) enhance the level of ICT literacy among the Staff.

ANNEX A

PROHIBITED CONDUCT UNDER ICT POLICY

The following provisions describe conduct prohibited under this Policy:

a) Altering system software or hardware configurations without authorization.

b) Disrupting or interfering with the delivery or administration of ICT resources.

c) Attempting to access or accessing another's accounts, private files, e-mail messages, or intercepting network communication without the owner's permission except as appropriate to your job duties.

d) Misrepresenting oneself as another individual in electronic communication.

e) Installing, copying, distributing, or using digital content (including software, music, text, images, and video) in violation of copyright and/or software agreements or applicable laws.

f) Engaging in conduct that interferes with others' use of shared ICT resources.

g) Using TBS ICT resources for commercial or profit-making purposes or to represent the interests of groups unaffiliated with TBS.

h) Ignoring individual departmental and system policies, procedures, and protocols.

i) Facilitating access to TBS ICT resources by unauthorized users.

j) Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose.

k) Knowingly using ICT resources for illegal activities. Criminal or illegal use may include obscenity, pornography, threats, harassment, copyright infringement, TBS trademark infringement, defamation, theft, identity theft, and unauthorized access.

ANNEX B

ICT ACCEPTABLE USE

The following are the guidelines on Acceptable Use of ICT equipment and systems:

B.1 GENERAL GUIDELINES

B.1.1 Monitoring

TBS may access and disclose all data or messages stored on its systems or sent over its electronic mail system. TBS reserves the right to monitor communication and data at any time, with or without notice, to ensure that its ICT facility is being used only for intended purposes. Also TBS reserves the right to disclose the contents of messages for any purpose at its sole discretion. It is the responsibility of the Management to monitor communication and data in TBS ICT network. No monitoring or disclosure shall occur without the direction of TBS management, unless otherwise stated.

B.1.2 Retrieval

Notwithstanding the organization's right to retrieve and read any e-mail messages, such messages shall be treated as confidential and accessed only by the intended recipient. TBS employees are not authorized to retrieve or read any e-mail messages that are not sent to them and shall not use password, access a file, or retrieve any stored information unless authorized to do so.

B.1.3 Passwords

Initial passwords are assigned by Management and shall not be given to other staff or persons outside TBS. Employees shall change the provided passwords as soon as possible using the instructions provided by the ICT staff. TBS reserves the right to override any employee-selected passwords and/or codes. It is the responsibility of each employee to provide the authorized ICT staff with any such codes or passwords to facilitate access as needed. Periodically, staff may be required to change their passwords. At no time should a TBS employee allow a temporary, contractor or another employee use of his/her login. In the case where an employee does provide another person access to his/her account, he/she will be responsible for the actions of the individual using his/her account. Passwords shall not be stored in computer data files, on the network, or be displayed openly at any workstation.

B.1.4 Message content

The e-mail system shall not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. Further, the system shall not be used to create any offensive or disruptive messages. Offensive messages include those which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. The organization’s Staff and Administrative Regulations shall be considered the prevailing authority in the event of possible misconduct.

TBS employees shall understand that any data or information on the system shall not be deemed personal or private. The e-mail system shall not be used to send (upload) or receive

(download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

B.1.5 Software usage

TBS employees shall use the standard software provided by the Bureau, or identify applications needed in the course of their work as approved by TBS Management. Staff members shall not download applications, demos or upgrades without the authority of the ICT and Documentation Manager. Employees shall use the standard e-mail system provided by TBS for official e-mail communications, and shall not install their own e-mail systems. Use of instant messaging programs, such as AOL Instant Messenger, Windows Live Messenger, etc., is prohibited unless otherwise approved by the Management.

B.1.6 Backup

All network data and file resources shall be backed up regularly. Data stored on the local PC drives is not routinely backed up, and as a result, important data and applications shall not be stored on the C: drives of these machines. Staff working on especially crucial information shall backup data to disks which can be supplied by the ICT Department. Computer users shall be responsible for ensuring that data stored on their local machines is backed up as required by the backup procedures.

B.1.7 Access to computers

TBS shall provide computer user accounts to all TBS staff. External people who are determined to be strategically important to TBS, such as temporary staff, volunteers, or contractors, shall also be provided user accounts as appropriate, on a case-by-case basis which shall be determined by the TBS Management. The employee managing temporary or contract staff assumes responsibility for the identification of access requirements and use of the account. Accounts shall be revoked on request by the user or manager or when the employee terminates employment with TBS.

B.1.8 Internet use

The internet shall be used for standardization, quality assurance and supporting activities only. Employees with internet access shall not access, view, download, or print pornographic or other sexually explicit materials. In addition, employees shall be mindful that there is no assurance that e-mail texts and attachments sent within TBS and on the internet shall not be seen, accessed or intercepted by unauthorized parties.

B.2 GUIDELINES ON SECURITY ISSUES

B.2.1 Security incidents

Any individual who has knowledge of a security incident shall report it as soon as possible to his or her supervisor for reporting on to the ICT Department. An example could be the introduction of a virus to a PC and/or the network, or network access by an unauthorized user.

B.2.2 Security weaknesses

B.2.2.1 Any individual who has knowledge of a security weakness shall report it as soon as possible to his or her supervisor for reporting on to the ICT Department.

Examples of security weakness:

a) A PC may be left unattended, logged into a system leaving a system open for another user or other locking procedure potentially allowing access by unauthorized users.

b) Inclusion of too many individuals in a system's administrator profile.

c) Lack of procedures for signing out laptops or other portable devices to individuals, potentially allowing unidentified and/or unauthorized use of the equipment.

B.2.2.2 A weakness does not have to be specifically ICT related. It could be windows left open close to portable equipment, or a PC monitor displaying potentially sensitive data positioned to face a window.

B.2.3 Security breaches

Any individual who has knowledge of a breach shall report it as soon as possible to his or her supervisor for reporting on to the ICT Department. This may be the result of a specific security incident, a security weakness, a violation of security policies or procedures or a combination of all three**.**

B.2.4 Security violations

B.2.4.1 Any individual who has knowledge of a security violation shall report it as soon as possible to his or her supervisor for reporting on to the ICT Department.

B.2.4.2 Violation of this policy shall include, but is not limited to, any act which

a) Exposes TBS to actual or potential monetary loss through the compromise of ICT security;

b) Involves the creation, processing or use of any data found to be inaccurate or invalid;

c) Involves the accessing, creation, processing or use of any data by unauthorized users;

d) Involves the disclosure of confidential and/or personal information, the unauthorized use of corporate data and/or the sending of defamatory information;

e) Involves the creation, use, downloading or transmitting of any data or other material for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body;

f) Involves unauthorized modification, installation or use of software.

ANNEX C

RESPONSIBILITIES AND IMPLEMENTATION MODALITIES

C.1 GENERAL RESPONSIBILITIES

C.1.1 All users of ICT systems are required to formally acknowledge receipt of the ICT Policy and that they have read and understood its content.

C.1.2 ICT and information security is the responsibility of TBS as a whole and consequently a responsibility of all members of staff and other authorized users.

C.1.3 This policy shall be approved and adopted by the Board of Directors.

C.1.4 Management shall be responsible for implementation of this policy.

C.1.5 All providers and users of ICT services shall ensure the security of ICT resources including integrity, confidentiality and availability of all data they create, process or use.

C.1.6 All TBS employees are required to sign an acknowledgement form before accessing the various ICT systems in use. The elements regarding acceptable use and security of TBS ICT resources shall help employees to better determine how to use these systems in light of their own and the organization's privacy and security concerns.

C.2 RESPONSIBILITIES OF THE ICT STEERING COMMITTEE

The ICT Steering Committee shall foresee ICT governance activities including the main role of providing leadership and aligning all ICT investments, decisions and initiatives with overall TBS objectives.

Specifically, the Committee shall:

a) develop and recommend strategic ICT issues and policies;
b) review and recommend on ICT project development plans;
c) provide advice and guidance on proposed ICT initiatives;
d) ensure that ICT initiatives embody the overall mission and objectives of the Bureau;
e) coordinate preparation of ICT Strategy;
f) ensure that the ICT Strategy is aligned with the Bureau's Corporate Plan;
g) propose standards for ICT systems, software and hardware; and
h) prepare quarterly report for presentation to Management;

C.3 COMPOSITION OF THE ICT STEERING COMMITTEE

The ICT Steering Committee shall be appointed by the Director General and shall be composed of the following members:

a) Any director as chairperson;
b) Head of ICT Section as Secretary;
c) Directors;
d) Managers;
e) Any member of staff or external member as the Director General may deem necessary.

BIBLIOGRAPHY

1. e-Government Strategy (2013)
2. Sustainable Development Goals (SDGs)
3. Ministry of Education and Vocational Training's Information and Communication Technology Policy for Basic Education (2007)
4. National ICT Policy (2003)
5. National Strategy for Growth and Reduction of Poverty (NSGRP) (Phase II: 2010/11 – 2014/15 (2010)
6. Tanzania Development Vision 2025
7. Tanzania Revenue Authority (TRA) ICT Policy