TANZANIA BUREAU OF STANDARDS

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) POLICY

EFFECTIVE DATE: 1ST FEBRUARY, 2010

TABLE OF CONTENTS

PREFACE

This Information and Communication Technologies (ICT) Policy serves as a guideline for ICT matters and is subject to review/amendment as need arises so as to cope with the prevailing environment.

The Policy shall be used alongside other relevant policies, regulations and directives on matters relating to ICT.

This Policy is effective from February 1, 2010.

LIST OF ACRONYMS/ABBREVIATIONS

AOL – American Online
CD – Compact Disc
CD ROM – Compact Disc Read Only Memory
ICT – Information and Communication Technologies
ID – Identification
PC – Personal Computer
TBS – Tanzania Bureau of Standards
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.

"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.

ICT POLICY

1 INTRODUCTION

The Tanzania Bureau of Standards (TBS) Information and Communication Technologies (ICT) Policy is comprised of Acceptable Use and Security elements.

TBS provides a variety of electronic communication systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of TBS and, as such, are intended to be used for job-related purposes only.

This policy shall be communicated to all TBS ICT staff and end users through the TBS website and during the induction process of new employees. In addition a copy of this document shall be obtained from the departmental managers.

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.

The ICT and Documentation Department shall maintain the ICT Policy on behalf of TBS. However, other departments shall develop procedures and controls to accommodate specific requirements so long as these procedures do not compromise corporate policy and controls. This policy is intended to guide the development of procedures for staff practice.

In order to remain relevant to both advances in ICT and end-user expectations, the policy shall be reviewed regularly and revised as appropriate and clearly dated.

2 PURPOSE OF ICT POLICY

This ICT Policy is aimed at:-

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

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

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.

3 PROHIBITED CONDUCT UNDER THIS 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.

4 ICT ACCEPTABLE USE

TBS has an obligation of informing its employees about the type of behavior it expects from those using ICT in the workplace and about the consequences for abusing the technologies.

An Acceptable Use element of this Policy is a tool for dissemination of this information to users of the organization's ICT resources.

The following are areas covered by the ICT Acceptable Use.

4.1 Monitoring

TBS shall provide the network, personal computers, electronic mail and other communication devices for staff use to support TBS functions of standardization and quality assurance including supporting activities. 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 ICT and Documentation Manager to monitor communication and data in TBS ICT network. No monitoring or disclosure shall occur without the direction of either the ICT and Documentation Manager or the TBS management, unless otherwise stated.

4.2 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.

4.3 Passwords

Initial passwords are assigned by the ICT and Documentation Manager 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.

4.4 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.

4.5 Software Usage

TBS employees shall use the standard software provided by ICT section, 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 or the ICT and Documentation Manager.

4.6 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 and Documentation Department. Computer users shall be responsible for ensuring that data stored on their local machines is backed up as required by the backup procedures.

4.7 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.

4.8 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.

5 ICT SECURITY

5.1 Network Security

5.1.1 ICT and Documentation Department shall monitor network security on a regular basis.

5.1.2 Adequate information concerning network traffic and activity shall be logged to ensure that breaches in network security can be detected.

5.1.3 ICT and Documentation Department shall also implement and maintain procedures to provide adequate protection from intrusion into TBS's computer systems from external sources.

5.1.4 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.

5.1.5 Staff shall not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

5.2 Network Access

5.2.1 Access to the network, and any equipment, application, database or other resource shall be by individual login – i.e. unique user name and password.

5.2.2 Non-TBS computing equipment shall only be used to access TBS network resources if authorized by the ICT and Documentation Department.

5.2.3 Each individual who is authorized to access TBS network shall be given a profile which limits his or her access to approved data, files and software.

5.2.4 Data stored on a computer's hard drive is not automatically backed up, and may be accessible to anyone switching on the PC. A computer hard drive is therefore not secure and shall be seen as a last resort and a temporary, short term solution. Similarly, data shall not be stored on non-TBS equipment.

5.2.5 Where a computer is shared by a number of users, it is essential for all users to log off the computer before leaving it. A 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.

5.2.6 Access to systems and applications is restricted according to the role and business requirements of each user.

5.2.7 Within a system or application, segregation of duties shall be implemented to prevent accidental or deliberate misuse. Duties or responsibilities which may give rise to a conflict of interest if carried out by the same individual must be separated.

5.2.8 In general, access rights comprise the functions of read, write, delete and execute and these are allocated to each user in respect of each system and application.

5.2.9 Established access rights must be reviewed twice yearly as a minimum 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.

5.2.10 Systems Administrator access allows full unrestricted rights to defined systems and applications for management purposes, including the creation and removal of system users. This level of access shall be kept to the minimum number of individuals required to enable day-to-day operation and emergency access in the event of a system failure. Systems Administrator access shall be via unique individual ID.

5.2.11 The use of privileges in systems and applications shall be allocated in a restricted and controlled manner. Privileges enable users to override some controls within a system, usually for system management purposes, and privileges shall be removed when no longer required.

5.2.12 Access to systems and applications by third parties, such as partner organizations or contractor or software maintenance/support personnel, shall be subject to authorization and compliance with the TBS ICT security element. Access by third parties shall be 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.

5.3 Physical Security

5.3.1 All hardware devices shall bear an identification number, which shall not be removed throughout the life of the device.

5.3.2 All desktop devices, e.g. PC, printer and scanner, shall have adequate precautions taken to protect them against theft and accidental damage in addition to environmental threats and hazards. All manufacturers' and suppliers' instructions and advice shall be followed.

5.3.3 Security precautions shall, in the first instance, concentrate on adequate building and setting of the device in the office, and then may extend to simple lock down devices attached to a desk.

5.3.4 Procurement of ICT hardware shall be coordinated by ICT and Documentation Department. This ensures that equipment in use across TBS is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

5.3.5 ICT and Documentation Department cannot guarantee installation, support or servicing of equipment purchased independently.

5.3.6 All desktop computer equipment shall be turned off when not being used for an extended period of time.

5.3.7 Equipment shall be 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.

5.3.8 When not in use all portable devices such as laptop computers shall be retained in a secure environment. This may include a lockable store cupboard with controlled access.

5.3.9 All portable devices shall be security marked as soon as they are received and then added to the appropriate inventory. The same shall be traceable.

5.3.10 When portable devices are taken off premises all users shall ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times, e.g. not left visible but locked away.

5.3.11 Records shall be maintained within each department detailing their portable devices including type, serial number and software available, and include provision for signing out and return.

5.3.12 All computer consumables (disks, etc) shall be retained in a secure environment wherever possible and issued only for TBS activities. Consumables shall not be used for private purposes.

5.3.13 Server rooms, data centres and all other secure or sensitive areas shall be subject to additional security measures including controlled and authenticated access.

5.4 PC Security

5.4.1 ICT Section shall configure all PC's with virus protection software, which shall not be removed or disabled by users.

5.4.2 Each employee shall be 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.

5.4.3 All data disks and files entering or leaving TBS shall be scanned for viruses.

5.4.4 Staff shall log out of the network and turn their computers off before leaving the office.

5.4.5 Staff shall log off the network when away from their desks for an extended period of time.

5.5 Installation of Software

5.5.1 Procurement of software shall be coordinated by ICT and Documentation Department and only legally licensed software shall be installed in TBS computers.

5.5.2 It is the responsibility of each user to ensure that the correct licensing arrangements are followed when installing software. However, this is assumed to be correct when installation is done by ICT and Documentation Department, who shall retain records relating to current licenses and software packages in use.

5.5.3 Appropriate action will be 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.

5.5.4 Modifications to existing software are generally discouraged, and in any case shall be processed through ICT Section and user departments and where appropriate be subjected to change control procedures.

5.6 Virus Prevention and Control

5.6.1 *Anti-Virus software*

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

5.6.1.2 The approved anti-virus shall be deployed on a server and installed remotely on client computers.

5.6.1.3 The anti-virus library definitions shall be updated at least once per day. Anti-virus shall be set to scan automatically all client computers and servers once per day.

5.6.2 *Virus prevention*

5.6.2.1 All software shall be checked for viruses before installation on any TBS device, including computers, laptops and other portable devices.

5.6.2.2 Where a CD ROM, USB memory stick or other storage media is used to transfer files, program or data, from one machine to another, it shall be virus checked before use, 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.

5.6.2.3 If there is any doubt as to the origin of the files being transferred, they shall always be checked for viruses before use.

5.6.3 *Downloading from the internet*

Files downloaded from the internet shall initially be 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.

5.6.4 *Extracting e-mail attachments*

5.6.4.1 If there is any doubt about the authenticity or content of an e-mail or its attachment the ICT and Documentation Department shall be contacted immediately for advice prior to opening the file.

5.6.4.1 If a virus is found, or suspected to be on a machine or external storage media, the ICT and Documentation Department shall be informed immediately.

5.6.4.1 ICT and Documentation Department shall notify users, through e-mail, concerning a particular virus and its effect. All users shall take appropriate action when so notified. Deliberate contravention of such a notification is a potential disciplinary matter.

5.7 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 and Documentation Department. An example could be the introduction of a virus to a PC and/or the network, or network access by an unauthorized user.

5.8 Security Weaknesses

5.8.1 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 and Documentation 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.

5.8.2 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.

5.9 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 and Documentation 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**.**

5.10 Security Violations

5.10.1 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 and Documentation Department.

5.10.2 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.

5.11 Sending Confidential Information

5.11.1 It is the responsibility of TBS employees to 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. It is also the responsibility of the employees to bring to the supervisors' attention any areas of concern regarding the transfer or transportation of such information.

5.11.2 Personal and sensitive corporate data shall not be disclosed, transferred, or copied to third parties without authorization from an appropriate senior officer, who understands the purpose of the request and is aware of the procedures to follow.

5.11.3 Before making information available to anyone else, employees shall make sure that they have the authority to disclose it.

5.11.4 Information shall never be given out over the phone or by any other verbal means unless it is absolutely clear to whom it is being given and that he/she is entitled to the information and is ready and able to accept it.

5.11.5 Care shall be taken to ensure that conversations involving confidential and/or personal information cannot be overheard.

5.11.6 E-mail is not a secure means of communication outside the security of the TBS's network and shall not be used for sending sensitive corporate data.

5.12 Disposal of Media and Equipment

5.12.1 PCs which have become obsolete or are surplus to requirement shall have their hard disks checked for content. Software that is being transferred to another machine shall be uninstalled and all data files shall be deleted.

5.12.2 Data storage devices shall be purged of sensitive data before disposal or securely destroyed.

5.13 Termination of employment

5.13.1 When a user who has network access leaves the employment of TBS the appropriate manager shall arrange for the transfer of any necessary files and e-mail folders.

5.13.2 On termination it is the user's responsibility to return all equipment, ID's, software, documentation (both paper and electronic) and any other TBS asset in his/her possession.

6 COMPLIANCE

Failure to comply with any component of the ICT Policy shall result into disciplinary action.

7 CORPORATE OBLIGATION

7.1 Infrastructure

7.1.1 *Network development and connectivity*

TBS shall 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.

7.1.2 *Physical infrastructure*

In line with its vision for ICT, TBS shall build a solid foundation of ICT infrastructure. Further, TBS shall establish a sound fiscal planning that shall guarantee the state-of-the-art maintenance of the infrastructure.

7.2 Equipment

7.2.1 *Acquisition and maintenance*

Adequate resources shall be made available for a regular maintenance of the ICT equipment (computers, servers etc). The ICT and Documentation Department shall put in place an elaborate programme of refurbishment and replacement of obsolete and outdated computer equipment. The ICT and Documentation Department shall also systematically modernize her stock of computers to meet the demands of latest software, web access, and other basic tasks of computation and communication. Equipment acquisition and maintenance shall be coordinated by the ICT and Documentation Department.

Maintenance programs shall be put in place to ensure that the hardware are serviced, repaired and replaced from time to time.

7.2.2 *Network equipment*

Network equipment availability is critical for the maintenance of TBS databases, backup and archiving services to ensure the provision of coherent service to users on their own machines. Adequate resources shall be made available.

7.2.3 *Power supply and equipment protection*

Uninterrupted power supply systems do not withstand rampant fluctuations and lightning induced surges. The ICT systems shall be protected from the devastating effects of lightning and larger electrical power switching transient over-voltages and surges**.** TBS shall invest in ICT system protection devices.

8 RESPONSIBILITIES

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

8.2 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.

8.3 This policy shall be approved and adopted by the Chief Executive Officer.

8.4 Departmental heads shall be responsible for implementation of this policy.

8.5 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.