

Vocational Education and Training Authority (VETA)

THE UNITED REPUBLIC OF TANZANIA

Applicable Public Institution
VETA

Document Title
Acceptable ICT Use Policy

Document Number
ICT USE POLICY V:1.0


PPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Pancras M.S. Bujulu	Director General		22/6/2021

Table of Contents

1. OVERVIEW	2
1.1. Introduction	2
1.2. Rationale	2
1.3. Purpose	2
1.4. Scope	2
2. ACCEPTABLE ICT USE POLICY STATEMENTS	3
2.1. Acceptable Behaviour	3
2.2. Unacceptable Behaviour	3
2.3. Acceptable use of ICT Assets	4
2.4. Acceptable Email Use	4
2.5. Internet and Intranet Usage	5
2.6. Use of Passwords and Authentication	7
2.7. Security of ICT Equipment	8
2.8. Mobile Devices Usage	9
2.9. Closed Circuit Television (CCTV) Usage	9
2.10. Access Cards	10
2.11. Software Use and Licensing	10
3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT	11
3.1. Implementation and Reviews	11
3.2. Exceptions	11
3.3. Roles and Responsibilities	11
3.4. Monitoring and Evaluation	11
4. GLOSSARY AND ACRONYMS	12
4.1. Glossary	12
4.2. Acronyms	12
5. RELATED DOCUMENTS	12
6. DOCUMENT CONTROL	12
APPENDIX	12
Declarations by Staff	12

1. OVERVIEW

1.1. Introduction

This document formalizes the policy for employees and stakeholders ("users") of **VETA** on the use of information and communication technology resources; including computers, printers and other peripherals, programs, data, local area network, video conference facilities, door access control, CCTV, intranet and the Internet. In addition to this document, additional rules governing the use of specific ICT Resources may be developed, e.g. network acceptable use guidelines. Use of **VETA** ICT Resources by any employee or third party shall constitute acceptance of the terms of this document and any such additional documents.

1.2. Rationale

The Acceptable ICT Use Policy enables users to understand what is considered acceptable and unacceptable in the use of **VETA** ICT resources. It sets out the required behaviors and actions when using **VETA** ICT equipment, Intellectual Property or software including incidental personal use of ICT systems, email addresses and the Internet (including social networking).

1.3. Purpose

The main purpose of this document is to set out how relevant stakeholders shall adhere to **VETA** policy for usage of ICT facilities and data. The specific objectives of this policy are:

- i. To ensure that **VETA** ICT facilities and services are used in an appropriate and responsible manner;
- ii. To ensure that appropriate password controls are implemented that address the risk of unauthorized access into the variety of Information and Communication Technology (ICT) facilities and services at **VETA**;
- iii. To safeguard the integrity and security of **VETA** ICT facilities and services; and
- iv. To ensure consistent understanding of staff members responsibilities when using the **VETA's** electronic messaging services.

1.4. Scope

These acceptable ICT use policy applies equally to all **VETA** employees, including permanent, temporary, part-time and contract employees, as well as learners, contractors, consultants, or any other third-parties who use ICT resources and ICT equipment owned, leased, or rented by VETA and includes use at home. It also applies to any person connecting personally owned equipment to the **VETA** network from any location.

2. ACCEPTABLE ICT USE POLICY STATEMENTS

2.1. Acceptable Behaviour

- 2.1.1. **VETA** believes that ICT resources empower users and make their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, employees and stakeholders are encouraged to use ICT resources to the fullest extent in pursuit of **VETA**'s goals and objectives.

2.2. Unacceptable Behaviour

- 2.2.1. Creation, display, production, down-loading or circulation of offensive material in any form or medium.
- 2.2.2. Failure to adhere with the terms and conditions of all license agreements relating to ICT facilities used including software, equipment, services documentation and other goods.
- 2.2.3. Deliberately introducing viruses, worms, trojan horses or other harmful or nuisance programs or file into any **VETA** ICT facility, or taking deliberate action to circumvent any precautions taken or prescribed by the institution.
- 2.2.4. Loading onto the ICT facilities any software without permission from the designated authority.
- 2.2.5. Removing or interfering with output of the ICT facilities belonging to another user.
- 2.2.6. Failure to note and report on any observed or suspected security incidents, security weaknesses or threats.
- 2.2.7. Allow non –**VETA** employee to use resources assigned to him/her without prior authorization.
- 2.2.8. Unless such use is reasonably related to a user's job, it is unacceptable for any person to use **VETA** ICT resources:
- i. in furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
 - ii. for any political purpose;
 - iii. for any commercial purpose;
 - iv. to send threatening or harassing messages, whether sexual or otherwise;
 - v. to access or share sexually explicit, obscene, or otherwise inappropriate materials;
 - vi. to infringe any intellectual property rights;
 - vii. to gain, or attempt to gain, unauthorized access to any computer or network;
 - viii. for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
 - ix. to intercept communications intended for other persons;
 - x. to misrepresent either **VETA** or a person's role at **VETA**;
 - xi. to distribute chain letters;
 - xii. to access online gambling sites; or
 - xiii. to libel or otherwise defame any person.

2.3. Acceptable use of ICT Assets

- 2.3.1. Users shall not disclose, or disseminate to unauthorized person, any information or data that they came across during system access.
- 2.3.2. Users shall not access or try to access information than what was granted to access.
- 2.3.3. Users shall ensure that any discarded information or data is properly disposed.
- 2.3.4. Users shall not upload any business files to personal Internet sites or via personal email/social media as they put the data out of **VETA** control and may result in leakage of confidential information.
- 2.3.5. Users shall not use any **VETA** ICT facilities for any personal activities that are prohibited under the law.
- 2.3.6. Messages, postings and blogs shall not disclose any proprietary or confidential information about **VETA** or **VETA's** clients, including client contract information, internal policies, standards, procedures, processes, guidelines or financial information.
- 2.3.7. Any comments or postings made regarding user's colleagues or other individuals shall not breach their rights, including the right to data privacy and any comments or postings shall not adversely affect **VETA** reputation.
- 2.3.8. Users shall not accept offers of software upgrades or security patches from pop-up windows that appear when browsing the Internet, as these often contain malware.
- 2.3.9. **VETA** shall not provide ICT support or backup arrangements for personal applications and downloads, and it shall provide any support to help manage employee personal files.
- 2.3.10. Any downloaded software, music or other data, which is for personal use, that is found to or is suspected of interfering with the performance of the **VETA's** computer/network or is inappropriately licensed shall be removed from the computer by **VETA's** ICT Team.
- 2.3.11. All users shall be given awareness training on the acceptable use of the institution's ICT assets by ICT Team.

2.4. Acceptable Email Use

- 2.4.1. Users shall not use their work email address for any non-work purposes which may reasonably be mistaken as being related to the organisation, e.g. correspondence with the media, registering domain names or ordering the supply of business-type goods (even if this is for delivery to your home address).
- 2.4.2. **VETA** reserve the right to inspect, monitor and disclose the contents of any email created, sent, received or forwarded by using the Institute computer network or email system.
- 2.4.3. Emails addressed to other Institutions or to individuals outside **VETA** must clearly identify the sender by full name, position and contact address at the Institute.
- 2.4.4. Use of VETA e-mail system for personal purposes is prohibited.

Vocational Education and Training Authority (VETA)

- 2.4.5. Users must ensure that the content and tone of their e-mail messages cannot be considered offensive or abusive or of a discriminatory or bullying nature or constituting harassment of any kind.
- 2.4.6. **VETA** employee shall not send chain emails addressed to larger user groups without approval.
- 2.4.7. Users must be careful when opening email attachments received from unsolicited senders, as this may contain malicious codes.
- 2.4.8. **VETA** employees are responsible for the content of emails sent from their email addresses.
- 2.4.9. Users must not spoof or otherwise falsify a sender address.
- 2.4.10. **VETA** employees are not authorised to try and gain access to another employee's data files and email without the consent of the latter.
- 2.4.11. Users are not permitted to send electronic mail that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or criticism of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- 2.4.12. Users must not use their email to distribute, disseminate or store images, text or materials that might be considered indecent, pornographic or illegal.
- 2.4.13. Users must not knowingly or purposely send emails containing computer viruses, worms, trojan horses, or any other form of malware that could damage or interfere with the **VETA** network or another user's computer.
- 2.4.14. **VETA** employees and related parties must not send unapproved chain letters, spam emails or pyramid emails to anyone at any time.
- 2.4.15. **VETA** employees and related parties must should refrain sending broadcast emails, i.e. they should avoid sending the same message to a large number of recipients unless absolutely necessary.
- 2.4.16. Users must avoid sending excessively large electronic mail messages or attachments.
- 2.4.17. Users must double-check the email addresses of recipients when forwarding email messages.
- 2.4.18. Users are strictly forbidden to open attachments received via email messages which are from unknown (if possible) or mistrusted sender(s).

2.5. Internet and Intranet Usage

- 2.5.1. Internet access shall be provided to users to support daily job activities
- 2.5.2. **VETA's** Internet service may not be used for transmitting, retrieving or storing of any communications or images which are pornographic.
- 2.5.3. Users shall not use the Internet to transmit any proprietary, confidential, or otherwise sensitive information without the proper controls.
- 2.5.4. Unless specifically authorized, on item by item basis, users are strictly prohibited to use the Internet for:
 - i. Downloading of games or shareware programs.
 - ii. Ordering (shopping) of personal items or services.
 - iii. Playing of any games or participating in any on-line contest or promotion.

Vocational Education and Training Authority (VETA)

- iv. Deliberately propagating computer viruses, worms, trojan horses or trap door.
 - v. Disabling or overloading any computer system or network or to attempt to disable, defeat or circumvent any system intended to protect the privacy or security of another user.
 - vi. Downloading or distributing pirated software or data.
- 2.5.5. All official internal publications will be posted on the Intranet once they have been approved by **VETA**.
- 2.5.6. The use of the Intranet is intended exclusively for the work undertaken for or by **VETA**.
- 2.5.7. Sensitive or confidential information must not be exchange via the Intranet.
- 2.5.8. Users should act responsibly and maintain the integrity of the data/information within the Intranet all the times.
- 2.5.9. All information/data posted to the Intranet should be checked for virus/bugs.
- 2.5.10. Internet usage activities of **VETA** staff may be monitored by the ICT team.
- 2.5.11. Users are expected to protect their personal user credentials, such as user IDs and passwords. These should in no case be given to anyone (including colleagues). These credentials shall not be stored on Internet browsers.
- 2.5.12. Users are not allowed to connect any personal devices on their workstations to access the Internet directly, except if provided/approved by the ICT **section** for a specific purpose.
- 2.5.13. **VETA** employees shall not access **VETA** confidential data via a public computer such as in a cybercafé.
- 2.5.14. It is strictly prohibited to download unapproved software using VETA Internet access and install same on **VETA** devices.
- 2.5.15. Users shall not use **VETA** Internet access to download movies, pictures and music files unless work related.
- 2.5.16. All downloaded files from the Internet should be scanned using dependable anti-virus detecting software before they are opened on **VETA** devices.
- 2.5.17. Users must not deliberately try to bypass security controls on **VETA** systems to access the Internet.
- 2.5.18. Users are not allowed to disable the anti-virus protection running on their computers for browsing the Internet.
- 2.5.19. Users shall not use the Internet facilities provided to them at work for sexual or racial harassment.
- 2.5.20. Users must not use the Internet provided at work to gain unauthorised access to other systems or web sites.
- 2.5.21. Users are forbidden from using file-sharing technologies, except those provided by the ICT on **section** at work.
- 2.5.22. Users of portable devices accessing the Internet from public places should make sure that proper security measures are maintained, such as not connecting to unsecured network.

Vocational Education and Training Authority (VETA)

2.6. Use of Passwords and Authentication

- 2.6.1. Granting of access rights to some **VETA** ICT facilities will be by the provision of secret authentication methods, commonly the username(s) and password(s), thus the **VETA** ICT facility users;
- i. Must not use another user's username or password, nor allow any password issued to them to become known to any other person.
 - ii. Must not leave ICT facilities unattended after logging in.
 - iii. Must notify the designated authority of any change in their status which may affect their right to use ICT facilities.
 - iv. Must ensure passwords used not based on personal information like family names, year of birth or login name.
 - v. Password must be alphanumeric, i.e. include numbers, upper and lower case
- 2.6.2. Users shall store their password as a clear text. Storing password in a computer file, whether on your hard drive or on disk, can make it accessible to unauthorised users.
- 2.6.3. Initial passwords that have been assigned as original user-ID passwords must be changed at the first user log-on, whether the information system forces them or not.
- 2.6.4. Passwords must never be written onto hard-copy surfaces, such as post-its, scratch papers, notepad, etc.
- 2.6.5. Password protected screen-savers on all PCs and servers must be implemented. The screen-savers must be automatically activated after at most five (5) minutes.
- 2.6.6. For systems that cannot have screen saver functionality, users must log off from their connection session when they plan to be away from their terminal.
- 2.6.7. When not turned off, PCs and terminals must be protected from unauthorised use by appropriate controls, such as key-lock, BIOS password, etc.
- 2.6.8. Computer users must create system passwords that are a minimum of eight (8) characters in length, and be comprised of letters, numbers, and special characters to the extent possible.
- 2.6.9. Users must be forced to change system passwords at most ninety (90) days. System Administrator/Head of ICT must enforce this through technical means by configuring password aging on systems. Where technically possible, user-ID access must be disabled upon thirty (30) days of inactivity (excluding super-user user-IDs).
- 2.6.10. Where technically feasible, new users must be forced by the system to change their initial password to one that meets password policy.
- 2.6.11. Passwords must not be visibly displayed on the screen when being entered.
- 2.6.12. Upon three (3) consecutive authentication failures, users must be locked out of the resource in which they are attempting to gain access, and must have to have their user-ID manually reset.
- 2.6.13. Connection sessions that are not active for more than thirty (30) minutes must automatically terminate both the application and network sessions. For those

Vocational Education and Training Authority (VETA)

systems that cannot automatically terminate sessions, password protected screen savers or terminal locks must be implemented.

- 2.6.14. All computers, databases or applications that store user-ID and password information must be secured in the strictest manner. Access to the user-ID tables must be restricted to only authorised persons.
- 2.6.15. Passwords must be stored on secure systems with a one-way encrypted algorithm.
- 2.6.16. All User ID and default passwords supplied by third parties must be changed following the installation of the software.
- 2.6.17. Users must log off from their connection session every time they complete their tasks.

2.7. Security of ICT Equipment

- 2.7.1. Users shall be responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use.
- 2.7.2. No equipment or other ICT facility shall be moved without the prior agreement of the designated authority.
- 2.7.3. No equipment may be connected in any way into the **VETA** supplied network or other ICT facility without authorization from ICT **section**.
- 2.7.4. In case of missing or stolen equipment, the user should immediately notify the Director General (DG) or Centre Manager and continue with proper measures to be taken. (This can be done through email or phone calls).
- 2.7.5. When ICT equipment is stolen, it must first be reported to the Police then other internal reporting processes will continue.
- 2.7.6. Users must take every precaution to avoid damage to equipment caused by eating or drinking in its vicinity.
- 2.7.7. The equipment must be switched off properly before leaving the office.
- 2.7.8. Users are not allowed to alter any software or hardware installation.
- 2.7.9. **VETA** equipment must not be taken off-site without prior authorisation.
- 2.7.10. Any equipment or media taken off the premises of **VETA** shall not be left unattended in public place. While travelling, users of portable devices are responsible for ensuring that proper physical handling is maintained. It is advisable to keep visual control over these devices at all times. For example, laptops should be carried as hand luggage and disguised where possible when travelling or laptops should not be left in back seats of cars as they can easily be stolen.
- 2.7.11. Users of **VETA** equipment in public areas shall take proper safeguards to ensure that unauthorised viewing of confidential or secret data is avoided, such as ensuring that their device is not left unattended, screens are locked when not in use and confidential information is not displayed on screens in public areas.
- 2.7.12. Off-premises laptops containing confidential information shall be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, so as to prevent unauthorised access.

Vocational Education and Training Authority (VETA)

- 2.7.13. Employees shall observe manufacturers' instructions for protecting equipment at all times, for example, necessary precautions should be taken to protect equipment against exposure to strong electromagnetic fields.
- 2.7.14. In the event that the user faces an operational or security incident he should immediately report it to the **Director General or Centre Manager** for proper handling and support.

2.8. Mobile Devices Usage

- 2.8.1. Mobile devices connected to the network should adhere to the following policies:
 - i. Their operating system and any installed software shall be fully patched and kept up to date.
 - ii. Up-to-date antivirus and antispyware protection shall be installed to provide protection from viruses, worms, trojan horses, disruptive programs or devices or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of **VETA** network.
 - iii. A personal firewall shall be installed to provide protection from unauthorized intrusions.
 - iv. The mobile device shall not have a blank password and all default passwords shall be changed.
- 2.8.2. All mobile devices (such as laptops, mobile phones, tablets) supplied by the Government or by **VETA** remain the property of **VETA** and usage of same shall therefore be monitored and audited.
- 2.8.3. Employees must take appropriate measures to protect the mobile devices against accidental loss, damage or theft.
- 2.8.4. Employees must immediately inform the **Director General or Centre Manager** when the device is stolen or lost to prevent unauthorised access to confidential information.
- 2.8.5. Users of mobile devices shall be directed to **the ICT Section** for installation of software application on their devices.
- 2.8.6. **VETA** network and system passwords must not be stored on mobile devices unless it is a system limitation.
- 2.8.7. Any mobile device no longer used by the user must be returned to the **ICT Section**.

2.9. Closed Circuit Television (CCTV) Usage

- 2.9.1. Materials or knowledge secured as a result of the use of CCTV systems shall not be used for any commercial purposes.
- 2.9.2. Any CCTV recorded data shall only be released for use in the investigation of a specific crime and with the written authority.
- 2.9.3. Daily management of CCTV system shall be the responsibility of the **ICT section**.
- 2.9.4. Access to the CCTV system and stored images shall be restricted to authorised personnel only.

Vocational Education and Training Authority (VETA)

- 2.9.5. Staff or visitors shall be granted access to the Control Room on a case-by-case basis and only then on written authorisation.
- 2.9.6. All staff working in the CCTV control room shall be made aware of the sensitivity of handling CCTV images and recordings.
- 2.9.7. Any complaints about **VETA's** CCTV system should be addressed to the ICT **section**.

2.10. Access Cards

- 2.10.1. Access control badges/cards will be issued by the **ICT Section** and remain the property of **VETA**.
- 2.10.2. **VETA** staff will obtain and display their access control badges/cards, while on the office and where all access is controlled.
- 2.10.3. **VETA** staff are forbidden to use access control badges/cards assigned to another person.
- 2.10.4. The protection of the access control badge/card is important responsibilities for each cardholder.
- 2.10.5. Any loss of staff access card should be immediately reported to ICT **VETA** and cost of new card should be taken by staff, who lost the card.
- 2.10.6. All the access control transactions records shall be maintained by ICT **VETA**.
- 2.10.7. Unauthorized locks or suspicious looking access controls must be reported to ICT **section** as soon as possible.

2.11. Software Use and Licensing

- 2.11.1. Only suitably licensed software may be used to perform the business of **VETA**. Any software installed on **VETA** ICT facilities for incidental personal use must also be suitably licensed.
- 2.11.2. **VETA's** resources or networks must not be used to acquire, copy, or distribute software, or other copyrighted material without appropriate licenses.
- 2.11.3. **VETA** retains the rights to applications and source codes developed during working hours on **VETA's** ICT facilities. This includes ICT applications developed for **VETA**, developed externally or paid for by **VETA**.
- 2.11.4. Users shall not install **VETA** licensed applications and software for use on non-**VETA** ICT facilities.
- 2.11.5. If personal use software or media files are found to interfere with the normal operation of **VETA's** systems or are considered to pose an unacceptable risk to the firm then they must be removed.
- 2.11.6. **VETA** will maintain a database of properly licensed software plus records of software licenses and proof of ownership in relation to Intellectual Property Rights maintained for business purposes.
- 2.11.7. **VETA** ICT will perform periodic scans of all PCs and mobile devices to identify installed software. Instances of software identified via periodic scanning of personal computers will be reconciled with licensing data and anomalies

Vocational Education and Training Authority (VETA)

addressed in a timely manner. Unlicensed software will be removed. Responsibility for such anomalies will be assumed to rest with the person to whom the PC is assigned.

- 2.11.8. Software applications that are no longer needed should be uninstalled so that the license can be made available for reassignment.

3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

3.1. Implementation and Reviews

- 3.1.1. This document shall come into operation once tabled and agreed in management meeting, and approved in its first page, and then shall be considered mandatory for all **VETA** business operations.
- 3.1.2. Failure to observe this policy may subject individuals to loss of ICT resources access privileges or to disciplinary action, including termination of employment or contract.
- 3.1.3. This document shall be reviewed within three years, or whenever business environment of **VETA** changes in a way that affects the current policy.

3.2. Exceptions

- 3.2.1. In case of any exceptions to this policy, it shall be thoroughly documented and follow through a proper channel of authorization using the same authority which approved this document.

3.3. Roles and Responsibilities

- 3.3.1. It is the responsibility of any person using **VETA's** ICT resources to read, understand, and follow these guidelines. In addition, users are expected to exercise reasonable judgement in interpreting these guidelines and in making decisions about the use of ICT resources. Any person with questions regarding the application or meaning of statements in this policy should seek clarification from ICT **section**.
- 3.3.2. The head responsible for ICT shall enforce compliancy by using audit trails and triggering access revocation/removal to **VETA** systems and networks.

3.4. Monitoring and Evaluation

- 3.4.1.1. ICT Steering Committee (or its equivalent body) shall meet regularly to monitor and evaluate the compliancy to **VETA's** acceptable ICT use policy.

Vocational Education and Training Authority (VETA)

4. GLOSSARY AND ACRONYMS

4.1. Glossary

Acceptable ICT Use Policy – A document that elaborate on the Public Institution's ICT Management Philosophy by outlining appropriate use of the Institution's Information, Communication and Technology resources and it applies to all users of ICT resources.

4.2. Acronyms

- **BIOS** – Basic Input/Output System
- **CCTV** – Closed Circuit Television
- **ICT** – Information & Communication Technology
- **ID** - Identification
- **PC** – Personal Computer

5. RELATED DOCUMENTS

- 5.1. ICT Policy
- 5.2. ICT Strategy
- 5.3. Enterprise Architecture
- 5.4. ICT Security Policy
- 5.5. ICT Service Management Guidelines
- 5.6. Disaster Recovery Plan
- 5.7. ICT Project Management Guidelines
- 5.8. ICT Acquisition, Development and Maintenance Guidelines

6. DOCUMENT CONTROL

VERSION	NAME	COMMENT	DATE
Ver. 1.0	ACCEPTABLE ICT USE POLICY		

APPENDIX

Declarations by Staff

These declarations have been designed to certify that users acknowledge that they are aware of **VETA**, Acceptable information and communication technology use policy and agree to abide by their terms.

I..... acknowledge that **VETA**, acceptable ICT use policy has been made available to me for adequate review and understanding. I certify that I have been given ample opportunity to read and understand it, and ask questions about my responsibilities on it. I am, therefore, aware that I am countable to all its terms and requirements; and that I shall abide by them. I also understand that failure to abide

Vocational Education and Training Authority (VETA)

by them; **VETA**, shall take against me appropriate disciplinary action or legal action, or both, as the case may be.

Signature:.....

Department/Unit:.....

Job Title:.....

Date: ____ / ____ / ____

-----For Government Control Only-----

Name: **Acceptable ICT Use Policy**

Reference: **eGA/EXT/SAM/003**

Version: **01**

Effective Date: **February 2016**

Creation: **eGovernment Agency**

Changes: **None**