# ENGINEERS REGISTRATION BOARD
# (ERB)

# ACCEPTABLE ICT USE POLICY
## (Draft)

MARCH, 2023

# ENGINEERS REGISTRATION BOARD ACCEPTABLE ICT USE POLICY

| APPROVAL | Name | Job Title/ Role | Signature | Date |
|---|---|---|---|---|
| Approved by | ENG. BERNARD KAVISHE | REGISTRAR | | 29/04/2023 |

Institution
**ENGINEERS REGISTRATION BOARD**

**Document Title**
Acceptable ICT Use Policy

**Document Number**

ERB/ICT/007/2023

TABLE OF CONTENTS

# 1. OVERVIEW

## 1.1. Introduction

This document formalizes the policy for employees and stakeholders ("users") of ERB on the use of information and communication technology resources; including but not limited to computers, printers and other peripherals, programs, data, local area network, video conference facilities, door access control, surveillance system, Intranet and the Internet. In addition to this document, additional rules governing the use of specific ICT Resources may be developed, such as network acceptable use guidelines. Use of ERB 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 using ERB ICT resources. It sets out the required behaviours and actions when using ERB ICT equipment, Intellectual Property or software, including incidental personal use of ICT systems, e-mail 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 ERB policy for usage of ICT facilities and data. The specific objectives of this policy are:

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

## 1.4. Scope

This acceptable ICT use policy applies equally to all ERB employees, including permanent, temporary, part-time and contracts' employees, and any other stakeholders (Engineers, Trainees, Consultants) who use ICT resources and ICT

equipment owned, leased, or rented by ERB and includes use at home. It also applies to any person connecting personally owned equipment to the ERB network from any location.

## 2. ACCEPTABLE ICT USE POLICY STATEMENTS

### 2.1. Acceptable Behaviour

ERB believes that ICT resources empower users and make their jobs more fulfilling by delivering better services at lower costs. As such, employees and stakeholders are encouraged to use ICT resources to the fullest extent to pursue ERB's goals and objectives.

### 2.2. Unacceptable Behaviour

2.2.1. Creation, display, production, downloading, uploading 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, systems, 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 ERB 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 an 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 – ERB employee to use resources assigned to him/her without authorization.

2.2.8. Unless such use is reasonably related to a user's job, it is unacceptable for any person to use ERB 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 ERB or a person's role at ERB ;
(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 an 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 other than what was granted to access.
2.3.3. Users shall ensure that any discarded information or data is properly disposed of.
2.3.4. Users shall not upload any business files to personal Internet sites or via personal e-mail/social media as they put the data out of ERB control and may result in leakage of confidential information.
2.3.5. Users shall not use any ERB 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 ERB or ERB's clients, including client contact information, internal policies, standards, procedures, processes, guidelines or financial information.
2.3.7. Any comments or postings made regarding the 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 ERB 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. ERB 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 ERB's infrastructures or is inappropriately licensed shall be removed from the respective devices by ERB ICT Unit.
2.3.11. All users shall be given awareness training on the acceptable use of the institution's ICT assets by ERB ICT Unit.

2.3.12. Any ICT Assets which are no longer in use must be returned to the ERB's ICT Unit.

## 2.4. Acceptable E-mail Use

2.4.1. Users shall not use their work e-mail address for any non-work purposes which may reasonably be mistaken as being related to the organization, such as 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. ERB reserve the right to inspect, monitor and disclose the contents of any e-mail created, sent, received or forwarded by using the Institute computer network or e-mail system.

2.4.3. E-mails addressed to other Institutions or individuals outside ERB must identify the sender by full name, position and contact address at the Institute.

2.4.4. Use of ERB e-mail system for personal purposes is prohibited.

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. ERB employee shall not send chain e-mails addressed to larger user groups without approval.

2.4.7. ERB employees and related parties must refrain from sending broadcast e-mails, such as they should avoid sending the same message to a large number of recipients unless necessary.

2.4.8. Users must be careful when opening e-mail attachments received from unsolicited senders, as this may contain malicious codes.

2.4.9. ERB employees are responsible for the content of e-mails sent from their e-mail addresses.

2.4.10. Users must not spoof or otherwise falsify a sender address.

2.4.11. ERB employees are not authorized to gain access to another employee's data files and e-mail without the latter's consent.

2.4.12. 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.

2.4.13. Users must not use their e-mail to distribute, disseminate or store images, text or materials that might be considered indecent, pornographic or illegal.

2.4.14. Users must not knowingly or purposely send e-mails containing computer viruses, worms, trojan horses, or any other form of malware that could damage or interfere with the ERB network or another user's computer.

2.4.15. ERB employees and related parties must not send unapproved chain letters, spam e-mails or pyramid e-mails to anyone at any time.

2.4.16. Users must avoid sending excessively large electronic mail messages or attachments.
2.4.17. Users must double-check the e-mail addresses of recipients when forwarding e-mail messages.
2.4.18. Users are strictly forbidden to open attachments received via e-mail messages 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. ERB's Internet service may not be used to transmit, retrieve, or store any communications or images that 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 an item by item basis, users are strictly prohibited from using 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 online contest or promotion.
(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 ERB.
2.5.6. The use of the Intranet is intended exclusively for the work undertaken for or by ERB
2.5.7. Sensitive or confidential information must not be exchanged 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. The ICT Unit may monitor the internet usage activities of ERB staff.
2.5.11. Users are expected to protect their 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 ERB's ICT Unit for a specific purpose.

2.5.13. ERB employees shall not access ERB confidential data via a public computer such as in a cybercafé.

2.5.14. It is strictly prohibited to download unapproved software using ERB Internet access and install same on ERB devices.

2.5.15. Users shall not use ERB 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 antivirus (preferably with Internet Security) detecting software before they are opened on ERB devices.

2.5.17. Users must not deliberately try to bypass security controls on ERB systems to access the Internet.

2.5.18. Users are not allowed to disable the antivirus 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 unauthorized access to other systems or web sites.

2.5.21. Users are forbidden from using file-sharing technologies, except those provided by the ERB 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 an unsecured network.

## 2.6. Use of Passwords and Authentication

2.6.1. Granting of access rights to some ERB ICT facilities will be by the provision of secret authentication methods, commonly the username(s) and password(s), thus the ERB 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 affecting 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, such as include numbers, upper and lower case

2.6.2. Users shall not store their password as cleartext. Storing password in a computer file, whether on your hard drive or on disk, can make it accessible to unauthorized 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, and the likes.

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. Users must log off from their connection session for systems that cannot have screen saver functionality when they plan to be away from their terminal.

2.6.7. When not turned off, PCs and terminals must be protected from unauthorized use by appropriate controls, such as key-lock, BIOS password, and the likes.

2.6.8. Computer users must create system passwords that are a minimum of eight (8) characters in length and comprise letters, numbers, and special characters to the extent possible.

2.6.9. For sensitive systems, 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 ageing 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 meet the password policy.

2.6.11. Passwords must not be visibly displayed on the screen when being entered.

2.6.12. For sensitive systems, 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. For non-sensitive system the users shall be allowed to retrieve their password upon following password recovery instructions.

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 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 authorized 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 to the ERB supplied network or other ICT facilities without authorization from ERB.

2.7.4. In case of missing or stolen equipment, the user should notify the Administration Department immediately and continue with proper measures to be taken. (This can be done through e-mail or phone calls).

2.7.5. When ICT equipment is stolen, one shall submit a loss report to ERB then other internal reporting processes will continue.

2.7.6. Users must take every precaution to avoid damage to the 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. ERB equipment must not be taken off-site without authorization.

2.7.10. Any equipment or media taken off the premises of ERB shall not be left unattended in a 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 ERB equipment in public areas shall take proper safeguards to ensure that unauthorized 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, such as passwords, smart cards, or encryption, to prevent unauthorized access.

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. If the user faces an operational or security incident, he should immediately report it to the Head of ICT unit 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 the ERB 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 ERB remain the property of ERB 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 ERB when the device is stolen or lost to prevent unauthorized access to confidential information.
2.8.5. Users of mobile devices shall be directed to ERB's ICT Unit for installation of software application on their devices.
2.8.6. ERB 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 ERB.

## 2.9. Security Surveillance Systems (such as CCTV Camera)

2.9.1. Materials or knowledge secured due to the use of surveillance systems shall not be used for any commercial purposes.
2.9.2. Any surveillance 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 the surveillance system shall be the responsibility of the ERB ICT Unit.
2.9.4. Access to the surveillance system and stored images shall be restricted to authorized personnel only.
2.9.5. Staff or visitors shall be granted access to the Control Room on a case-by-case basis and only then on the written authorization.
2.9.6. All staff working in the surveillance system control room shall be made aware of the sensitivity of handling surveillance images and recordings.
2.9.7. Any complaints about ERB's surveillance system should be addressed to the ERB ICT Unit.

## 2.10. Access Control

2.10.1. Access control facilities (badges/cards) will be issued by the ERB and remain the property of ERB.
2.10.2. ERB staff will obtain and display their access control facility (badges/cards), while in the office and where all access is controlled.
2.10.3. ERB staffs are forbidden to use access control badges/cards assigned to another person.
2.10.4. The protection of the access control facility (badges/cards) is an essential responsibility for each cardholder.
2.10.5. Any loss of staff access control facility (badges/cards), should be immediately reported to ERB ICT Unit, and the cost of the new card should be taken by staff who lost the card.
2.10.6. ERB ICT Unit shall maintain all the access control transactions records.
2.10.7. Unauthorized locks or suspicious-looking access controls must be reported to ERB ICT Unit as soon as possible.

## 2.11. Software Use and Licensing

2.11.1. Licensed software, including Open Source, may be used to perform the business of ERB. Any software installed on ERB ICT facilities for incidental personal use must also be licensed.
2.11.2. ERB's resources or networks must not be used to acquire, copy, or distribute software, or other copyrighted material without appropriate licenses.
2.11.3. ERB retains the rights to applications and source codes developed during working hours on ERB's ICT facilities. This includes ICT applications developed for ERB, developed externally or paid for by ERB.
2.11.4. Users shall not install ERB licensed applications and software for use on non-ERB ICT facilities.
2.11.5. If personal use software or media files are found to interfere with the normal operation of ERB's systems or are considered to pose an unacceptable risk to the firm, they must be removed.
2.11.6. ERB 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. ERB ICT Unit will perform periodic scans of all PCs to identify installed software. Instances of software identified via periodic scanning of personal computers will be reconciled with licensing data and anomalies addressed promptly. 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 after being agreed and approved by Executive Management Team and tabled to the Board of Directors, and shall be considered mandatory for all ERB business operations.

3.1.2. Failure to observe this policy may subject individuals to loss of ICT resources, access privileges, or disciplinary action.

3.1.3. This document shall be reviewed within five years or whenever the business environment of ERB changes to affect the current policy.

### 3.2. Exceptions

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

### 3.3. Roles and Responsibilities

3.3.1. It is the responsibility of any person using ERB's ICT resources to read, understand, and follow these guidelines. Besides, users are expected to exercise reasonable judgment in interpreting these guidelines and making decisions about using ICT resources. Any person with questions regarding the application or meaning of statements in this policy should seek clarification from ICT Unit.

3.3.2. The head of ICT Unit shall enforce compliancy by using audit trails and triggering access revocation/removal to ERB systems and networks.

### 3.4. Monitoring and Evaluation

The ICT Steering Committee shall meet quarterly to monitor and evaluate the compliance to ERB's acceptable ICT use policy.

## 4. GLOSSARY AND ACRONYMS

### 4.1. Glossary

**Acceptable ICT Use Policy** –A document that elaborates 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
- **ERB -** Engineers Registration Board

## 5. RELATED DOCUMENTS

5.1. ICT Policy
5.2. ICT Security Policy
5.3. Disaster Recovery Plan
5.4. ICT Project Management Guidelines
5.5. ICT Acquisition, Development and Maintenance Guidelines
5.6. ERB Staff Regulations

## 6. DOCUMENT CONTROL

| VERSION | NAME | COMMENT | DATE |
|---|---|---|---|
| Ver. 1.0 | ICT Unit | Initial Draft Submitted | |

## APPENDIX

### Declarations by Staff

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

I……..…… acknowledge that ERB 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. 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 by them, ERB shall take against me appropriate disciplinary action or legal action, or both, as the case may be.

Signature:…….

Department/Unit:…….

Job Title:……..

Date: ____ / __ / ____