ENGINEERS REGISTRATION BOARD
(ERB)

ICT SECURITY POLICY

(Draft)

MARCH, 2023

ENGINEERS REGISTRATION BOARD ICT SECURITY POLICY

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	ENG. BERNARD KAVISHE	REGISTRAR		19/04/2023

Applicable Public Institution
ENGINEERS REGISTRATION BOARD

Document Title
ICT Security Policy

Document Number

ERB/ICT/004/2023

Contents

1.0 OVERVIEW 3
1.1 Introduction 3
1.2 Rationale 3
1.3 Purpose 3
1.4 Scope 3
2.0 ERB ICT SECURITY POLICY STATEMENTS 4
2.1 ICT Security Governance and Management 4
2.2 ICT Security Operations 5
2.3 Security of ICT Assets 7
2.4 Identity and Access Management 8
2.5 ICT Security Incident Management 9
2.6 Information Systems Continuity Management 10
2.7 Security of ICT Acquisition, Development and Maintenance 11
2.8. Human Resource Security 12
2.9. Physical and Environmental Security 13
3.0. IMPLEMENTATION, REVIEWS AND ENFORCEMENT 15
3.1. Implementation and Reviews 15
3.2. Exceptions 15
3.3. Roles and Responsibilities 15
3.4. Monitoring and Evaluation 16
4.0. GLOSSARY AND ACRONYMS 17
4.1. Glossary 17
4.2. Acronyms 17
5.0. RELATED DOCUMENTS 17
6.0. DOCUMENT CONTROL 17

ENGINEERS REGISTRATION BOARD ICT SECURITY POLICY

1.0 OVERVIEW

1.1 Introduction

ERB information and technology assets are highly valuable and must be closely safeguarded. ERB operate within an increasingly electronic, interconnected, and regulated environment that necessitates a consistent and standardized approach to securing technology and information assets.

To ensure the continued protection of ERB information and to maintain a secure environment, the management team of ERB strongly believes that an ICT security approach aligned with local and international standards is necessary.

1.2 Rationale

It is the mandate of ERB that the information assets are protected from all types of threat, whether internal or external, deliberate or accidental, such that:

- Confidentiality of information is maintained;
- Integrity of information can be relied upon;
- Information is available when the business needs it; and
- Relevant statutory, regulatory, and contractual obligations are met.

1.3 Purpose

This ICT Security Policy is the cornerstone of ERB ICT security program and strategy, aimed at securing the information assets of the institution. It is also the purpose of this document to outline the roles and responsibilities of relevant stakeholders that implement the security controls.

1.4 Scope

This policy is applicable to all employees, contractors, consultants, temporary and other workers at ERB including all personnel affiliated with external parties must adhere to this policy. This policy is applicable to information assets owned or leased by ERB or to devices that connect to ERB network or reside at ERB sites.

2.0 ERB ICT SECURITY POLICY STATEMENTS

2.1 ICT Security Governance and Management

2.1.1 Management and Direction for ICT Security

2.1.1.1. There shall be an ICT Security Governance Committee which may have members not necessarily limited to ERB staff.

2.1.1.2. Single Point of Contact (SPOC) for ICT security Matters shall be appointed.

2.1.1.3. There shall be an ICT Security Strategy.

2.1.1.4. ERB shall allocate sufficient resources for effective ICT security management.

2.1.2. ICT Security Risk Management

ERB shall integrate ICT security risk management that include risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and evaluation into the Enterprise Risk Management Framework.

2.1.3. ICT Security Policies

ERB shall define a set of policies for ICT security, which shall be approved by Executive Management Team, published and communicated to employees and relevant external parties.

2.1.4. Review of the ICT Security Policies

The ICT security policies shall be reviewed at planned intervals or if significant Changes occur, to ensure their continuing suitability, adequacy and Effectiveness.

2.1.5. ICT Security Roles and Responsibilities

ERB shall define and allocate all ICT security responsibilities.

2.1.6. Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Institution's ICT assets.

2.1.7. Contact with Authorities

ERB shall maintain appropriate Contacts with relevant authorities.

2.1.8. ICT Security in ICT Project Management

ERB shall ensure that ICT security is addressed in ICT related projects.

2.1.9 Mobile Devices and Teleworking

2.1.9.1. ERB shall adopt a policy and supporting ICT security measures to manage the risks relating to mobile devices.

2.1.9.2. ERB shall implement a policy and supporting ICT security measures to protect information accessed, processed or stored at teleworking sites.

2.2 ICT Security Operations

2.2.1. Documented Operating Procedures

Operating procedures shall be documented and made available to all users who need them.

2.2.2. Change Management

Changes to the organization, business processes, information processing Facilities and systems that affect ICT security shall be controlled.

2.2.3. Capacity Management

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

2.2.4. Separation of Development, Testing and Operational Environments

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.2.5. Protection from Malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

2.2.6. Information Backup

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed Backup policy.

2.2.7. Event Logging

Event logs recording user activities, exceptions, faults and ICT security events shall be produced, kept and regularly reviewed.

2.2.8. Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

2.2.9. Administrator and Operator Logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

2.2.10. Clock Synchronization

The clocks of all relevant information processing systems within **ERB** shall be synchronized to a single reference time source.

2.2.11. Installation of Software on Operational Systems

Procedures shall be implemented to control the installation of software on Operational systems.

2.2.12. Management of Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, ERB exposure to such vulnerabilities evaluated and appropriate Measures taken to address the associated risk.

2.2.13. Restrictions on Software Installation

A policy governing the installation of software by users shall be established and implemented.

2.2.14. Information Systems Audit Controls

ICT audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to Business processes.

2.2.15. Network Controls

Networks shall be managed and controlled to protect information in systems and applications.

2.2.16. Security of Network Services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, irrespective of whether these services are provided in-house or outsourced.

2.2.17. Segregation in Networks

Groups of information services, users and information systems shall be Segregated on networks.

2.2.18. Information Transfer Policy and Procedures

Formal transfer policy, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

2.2.19. Agreements on Information Transfer

Agreements shall be signed with relevant stakeholders to address the secure transfer of business information between the organization and external parties.

2.2.20. Electronic Messaging

Information involved in electronic messaging shall be appropriately protected.

2.2.21. Confidentiality and Non-Disclosure Agreements

Requirements for confidentiality or non-disclosure agreements reflecting the ERB needs for the protection of information shall be identified, regularly reviewed and documented.

2.3 Security of ICT Assets

2.3.1. Inventory of ICT Assets

ICT assets associated with information and information processing facilities at ERB shall be identified and an inventory of these assets should be drawn up and maintained.

2.3.2. Ownership of ICT Assets

ICT assets maintained in the inventory shall be owned by the relevant Function or person at ERB.

2.3.3. Acceptable Use Policy for ICT Assets

Acceptable use policy of information, assets associated with information and information processing facilities shall be identified, documented and implemented.

2.3.4. Return of ICT Assets

All employees of ERB and external party users must return all ERB ICT assets in their possession to the Head of Administration and to inform the ICT Unit upon termination of their employment, contract or Agreement.

2.3.5. Classification of Information

Information shall be classified in terms of legal requirements, value, and criticality and sensitivity to unauthorized disclosure or modification.

2.3.6. Labeling of Information

An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by ERB.

2.3.7. Handling of ICT Assets

Procedures for handling ICT assets shall be developed and implemented in

accordance with the information classification scheme adopted by ERB.

2.3.8. Management of Removable Media

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by ERB.

2.3.9. Disposal of Media

Media shall be disposed off securely when no longer required, using the formal procedures established at ERB as per government directives.

2.3.10. Physical Media Transfer

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation in and out of ERB.

2.3.11. Cryptographic Controls

ERB shall develop and implement cryptographic controls for protection of information and information processing facilities.

2.4 Identity and Access Management

2.4.1. Access Control Policy

Access Control Policy shall be established documented and reviewed based on business and ICT security requirements of ERB.

2.4.2. Access to Networks and Network Services

Users at ERB shall only be provided with access to the network and network services that they have been Specifically authorized to use.

2.4.3. User Registration and De-registration

A formal user registration and de-registration process shall be implemented at ERB to enable and disable Assignment of access rights.

2.4.4. User Access Provisioning

A formal user access provisioning process shall be implemented at ERB **to** assign and revoke access rights for all user types to all systems and services.

2.4.5. Management of Privileged Access Rights

The allocation and use of privileged rights shall be restricted and controlled.

2.4.6. Management of Secret Authentication Information of Users

The allocation of secret authentication information shall be controlled through a formal management process.

2.4.7. Review of Access Rights

All ICT asset owners at ERB shall review users' access rights at regular intervals.

2.4.8. Removal or Adjustment of Access Rights

The access rights of all staff at ERB and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

2.4.9. Information Access Restriction

Access to information and application system functions shall be restricted in accordance with the Access Control Procedure of ERB

2.4.10. Secure Log-on Procedures

Where required by the Access Control Procedure, access to systems shall be controlled through a secure log-on procedure.

2.4.11. Password Management System

Password management systems must be interactive and must ensure usage of strong passwords.

2.4.12. Use of Privileged Utility Programs

The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.

2.4.13. Access Control to Program Source Code

Access to program source code shall be restricted.

2.5 ICT Security Incident Management

2.5.1. Responsibilities and Procedures

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

2.5.2. Reporting ICT Security Events

ICT security events shall be reported through appropriate management channels as quickly as possible.

2.5.3. Reporting ICT Security Weaknesses

Employees and other stakeholders using the ERB information systems and services shall be required to note and report immediately after any observed or suspected ICT security Weaknesses in systems or services.

2.5.4. Assessment of and Decision on ICT Security Events

ICT security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

2.5.5. Response to ICT Security Events

ICT security incidents shall be responded to in accordance with the documented procedures.

2.5.6. Learning from ICT Security Incidents

Knowledge gained from analyzing and resolving ICT security incidents shall be used to reduce the likelihood or impact of future incidents.

2.5.7. Collection of Evidence

ERB shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

2.6 Information Systems Continuity Management

2.6.1. Planning ICT Security Continuity

ERB shall determine its requirements for ICT security and the continuity of ICT security management in adverse situations, e.g, during a crisis or disaster.

2.6.2. Implementing ICT Security Continuity

ERB shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for ICT security during an adverse situation.

2.6.3. Verify, Review and Evaluate ICT Security Continuity

ERB shall verify the established and implemented ICT security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

2.6.4. Availability of Information Processing Facilities

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

2.7 Security of ICT Acquisition, Development and Maintenance

2.7.1. ICT Security Requirements Analysis and Specification

The ICT security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

2.7.2. Securing Application Services on Public Networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

2.7.3. Protecting Application Services Transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

2.7.4. Secure Development Policy

A policy for secure development of software and systems shall be established and applied to developments within the organization.

2.7.5. System Change and Control Procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

2.7.6. Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or ICT security.

2.7.7. Restrictions on Changes to Software Packages

Modifications to software packages shall be discouraged, limited to necessary Changes and all changes should be strictly controlled.

2.7.8. Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, Maintained and applied to any information system implementation efforts.

2.7.9. Secure Development Environment

ERB shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

2.7.10. Outsourced Development

ERB shall supervise and monitor the activity of outsourced system development.

2.7.11. System Security Testing

Testing of security functionality shall be carried out during development.

2.7.12. System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new Information systems, upgrades and new versions.

2.7.13. Protection of Test Data

Test data shall be selected carefully, protected and controlled.

2.8. Human Resource Security

2.8.1. Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and perceived risks.

2.8.2. Terms and Conditions of Employment

The contractual agreements with employees and contractors shall state the employee's and ERB responsibilities for information security.

2.8.3. Management Responsibilities

Management shall require all employees and contractors to apply information security in accordance with the established policy of ERB.

2.8.4. ICT Security Awareness, Education and Training

All employees of ERB, contractors and consultant shall receive appropriate awareness education and training and regular updates in ERB ICT Security Policy, as relevant to their job function.

2.8.5. Disciplinary Process

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an ICT security breach.

2.8.6. Termination or Change of Employment Responsibilities

ICT security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to all employees and other stakeholders of ERB, and shall be enforced.

2.9. Physical and Environmental Security

2.9.1. Physical Security Perimeter

Security perimeters shall be defined and used to protect information processing facilities and areas that contain either sensitive or critical information.

2.9.2. Physical Entry Controls

Secured areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

2.9.3. Securing Offices, Rooms and Facilities

Physical security for offices, rooms and facilities shall be designed and applied.

2.9.4. Protecting Against External and Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

2.9.5. Working in Secure Areas

ERB shall design and apply procedures for working in secure areas.

2.9.6. Delivery and Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

2.9.7. Equipment Sitting and Protection

Equipment shall be identified and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

2.9.8. Supporting Utilities

Equipment shall be protected from power failures and other disruptions Caused by failures in supporting utilities.

2.9.9. Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

2.9.10. Equipment Maintenance

Equipment shall be properly maintained to ensure its continued availability and integrity.

2.9.11. Off-premises of ICT Assets

Equipment, information or software shall not be taken off-site without prior authorization.

2.9.12. Security of Equipment and Assets Off-premises

Security shall be applied to off-site ICT assets taking into account the different risks of working outside ERB premises.

2.9.13. Secure Disposal or Re-use of Equipment

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

2.9.14. Unattended User Equipment

Users at ERB shall ensure that unattended equipment has appropriate protection.

2.9.15. Clear Desk and Clear Screen Policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

2.10. ICT Security Compliance and Audit

2.10.1. Identification of Applicable Legislation and Contractual Requirements

All relevant legislative statutory, regulatory, contractual requirements and the ERB approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and for ERB.

2.10.2. Intellectual Property Rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual Property rights and use of proprietary software products.

2.10.3. Protection of Records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

2.10.4. Privacy and Protection of Personally Identifiable Information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

2.10.5. Independent Review of ICT Security

ERB approach to managing information security and its implementation (such as control objectives, controls, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

2.10.6. Compliance with ERB ICT Security Policy

ERB shall ensure that regular reviews are done, on the compliance of information processing and procedures with the appropriate ERB ICT Security Policy and any other ICT security requirements.

2.10.7. Technical Compliance Review

Information systems shall be regularly reviewed for compliance with the **ERB information** security standards and guidelines.

3.0. 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 then shall be considered mandatory for all ERB operations.

3.1.2. ERB staff found to have violated this policy may be subject to disciplinary action in accordance with rules defined by ERB staff regulations.

3.1.3. This document shall be reviewed within five years, or whenever business environment of ERB changes in a way that affects the current policy.

3.2. Exceptions

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. **Registrar**

3.3.1.1. Shall be the overall Authority for the ICT Security Management of the ERB.

3.3.1.2. Shall be the chair of ICT Security Governance Committee, the task which may be delegated.

3.3.1.3. Shall find a suitable method for selecting the ICT Security Secretary, most likely the institution's Single Point of Contact for ICT Security.

3.3.2. ICT Security Governance Committee

3.3.2.1. Shall comprise of permanent members from Executive Management Team or May be the Management Team Sitting with a focus on ICT Security Matters.

3.3.2.2. Shall develop ICT Security Strategic Plan for the ERB.

3.3.2.3. Shall identify current and future ICT Security technology needs for the ERB.

3.3.2.4. Shall monitor and evaluate ICT Security Achievements against ICT Security Strategic Plan.

3.3.2.5. Shall provide advice and recommendations to Registrar /Executive Management on pressing ICT Security Matters affecting the ERB.

3.3.3. ICT Security Governance Committee Secretary

3.3.3.1. Shall be responsible for overseeing implementation of ICT Security plans of the ERB

3.3.3.2. Shall coordinate and advice Management about the implementations of ICT Security Strategic Plans.

3.3.3.3. Shall be a permanent member of ICT Security Governance Committee for his/her duration of appointment.

3.3.3.4. Shall receive inputs from ICT Security Operations Meeting for coordinating the executions of agreed plans.

3.3.4. Head of Departments and Units

3.3.4.1. Shall be responsible for implementation of ICT Security plans falling under areas of their responsibilities through coordination and liaising with ICT Security Secretary.

3.3.4.2. Shall be members of ICT Security Operations meetings where the Accounting Officer of ERB shall be the chairperson.

3.3.4.3. Head of departments and Units shall supervise all ICT Security issues falling under their areas of responsibilities for execution.

3.3.5. Employees

3.3.5.1. All employees of ERB shall have basic ICT security awareness training, any suspicious issue related to ICT security to the relevant authorities.

3.3.5.2. Employees from different departments/units shall be selected as members of Quarterly ICT Security Operations Meeting.

3.3.5.3. The selected employees shall be champions in ICT Security matters regarding the ERB.

3.4. Monitoring and Evaluation

3.4.1.1. ICT Security Governance Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT Security as per ERB ICT Security Strategic Plan.

4.0. GLOSSARY AND ACRONYMS

4.1. Glossary

ERB ICT Security Policy – A document that elaborate on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the ICT Security Management Framework, commonly known as ERB ICT Security Policy of an Institution.

4.2. Acronyms

ICT – Information & Communication Technology
SPOC – Single Point of Contact
ERB **-** Engineers Registration Board

5.0. RELATED DOCUMENTS

5.1. ICT Policy
5.2. ICT Strategy
5.3. ICT Service Management Guidelines
5.4. Disaster Recovery Plan
5.5. Acceptable ICT Use Policy
5.6. ICT Project Management Guidelines
5.7. ERB Staff Regulation
5.8. ICT Acquisition, Development and Maintenance Guidelines

6.0. DOCUMENT CONTROL

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