REB institutional ICT Policy

Table of Contents

1. Introduction

The use and maintenance of information and communication technology (ICT) hardware, software and data requires discipline and rigid rules to ensure the existence of the highest levels of consistency and control. It is for this purpose that Rwanda Education Board (REB) has developed ICT Policy.

2. Scope

This policy applies to the management of ICT infrastructure and systems in REB, hereinafter referred to as the ICT and is approved by REB Senior Management.

3. Objective

This ICT policy will lead the elaboration, management and utilization of REB ICT infrastructure and systems. It will serve as a guide and reference to acquire, use and develop ICTs and related services at all operational levels within REB.

This ICT policy is categorized in the following areas:

- ICT Standards
- ICT Related Project Management
- Acquisition
- Applications Development
- Software Licensing
- Change Control
- ICT Asset Management
- ICT Asset Disposal
- Access control and user account management
- Password Usage and Management
- Physical and Environmental security
- Information Classification
- Backup and Disaster Recovery
- Email and Internet

4. Policy areas

4.1 ICT Standards

- Identify appropriate ICT standards and advise users and departments on the application standards.
- All procurement and acquisitions of ICT equipment and systems must follow ICT Standards and refer to technical specifications from ICT Unit.

- ICT Unit will regularly update ICT standards to meet REB needs.
- ICT Standards must be continually communicated.
- ICT Unit will be responsible for the follow up of the implementation of ICT standards.

4.2 ICT Related Project Management

- All ICT related projects, regardless of size, scope or value, should be designed to achieve the REB vision and missions.
- ICT related projects must have clear goals, scope, requirements and activity/implementation schedule before execution.
- ICT related projects must be formally documented from initiation through execution for sustainable continuation and ownership.
- Any changes within the project must be formally documented and approved through a formal change management process.
- At closure, all projects must be formally handed over to the respective beneficiary department and ICT Unit, with all the solution/product documentation including project management documentation.
- Management of warranty and guarantees must be carried out for all projects.

4.3 Acquisition

- Purchase of new hardware, software and ICT services must be done in accordance with Government of Rwanda' Procurement policies and procedures.
- Any request for new hardware, software or ICT services should take into consideration REB business plan through ICT unit.
- Technical analysis must be conducted to ensure that proposed ICT request is aligned with technical specifications and REB requirements.
- REB should meet licensing requirements in order to avoid the usage of any counterfeit software.
- Third-party software maintenance agreements must be implemented where necessary to ensure that software updates will be available within agreed timeframes in case of bug fixes or changes required.

4.4 Applications Development

- The development of all applications must follow a defined software development life cycle (SDLC).

- Impact assessment of new hardware and applications on an ICT environment should be conducted before deployment, tuning and integration.
- Applications development should contain a testing plan, user procedures and operations manuals.
- Applications development should define an implementation plan encompassing roll-out/installation procedures, troubleshooting, distribution control, storage, as well as handover from testing to production.
- A training program for administration, technical team and end users should be part of all applications development.

4.5 Software Licensing

- Only software for which a legal contract exists may be installed onto REB ICT assets.
- When a software contract expires and is not to be renewed, the software must be de-installed, and all terms and conditions of the contract adhered to.
- Licensed software or related documentation may not be duplicated for use either on REB premises or elsewhere unless REB is expressly authorized to do so by agreement with the licensor and if this is approved by the relevant ICT manager.
- Software may not be loaned to any user or contractor unless expressly authorised to do so by agreement with the licensor and if this is approved by the relevant ICT manager.
- Software on multiple machines may only be installed in accordance with the applicable license agreement.
- A register of software and the software licensing details must be maintained and updated on a regular basis.
- All employees must adhere to the software licensing agreement.
- No Shareware or Freeware may be loaded onto REB ICT assets without the permission of the relevant ICT manager.

4.6 Change Control

- All changes to the ICT environment must follow a formal change management process that ensures that all changes requests to applications, procedures, processes and platforms are handled in a standardised manner.
- All requests for change must be assessed in a structured manner for all possible impacts to the overall ICT environment.
- Changes must be categorised and prioritised but urgent changes may follow separate formal procedures.

- Changes must follow a defined change approval process with defined authorities in the change management process.
- A register of changes must be maintained for all changes to the ICT environment.

4.7 ICT Asset Management

- REB ICT assets must be managed across their full lifecycle encompassing acquisition, redeployment, storage and disposal.
- An inventory of all REB ICT assets including hardware such as servers, workstations, laptops, modems, switches, routers, firewalls, printers must be maintained and kept up-to-date. An initial baseline must be developed containing all REB ICT assets and compared regularly against a physical inventory of REB ICT assets to identify changes.
- Any request to take ICT equipment out of the office must be approved by the Director of ICT Unit.
- Personal equipment shall not be brought and used on REB network or for REB business purposed, unless with prior express permission by the Director ICT.

4.8 ICT Asset Disposal

- In order to prevent the deterioration in the productivity of REB ICT assets, coupled with unacceptable high maintenance costs, a minimum lifespan is allocated to the different categories of these assets:

Description of Asset	**Expected Lifespan**
Desktop PC's, Laptops, CD ROM, CD RW, Audio equipment, monitors, disc drives	4 years
Printers, Scanners, Modems	4 years
Servers, mini or mid-range computers	5 years
Desktop software, operating systems	4 years

- It must be noted that these are the minimum terms and that each decision to retire an ICT asset must be viewed in terms of the residual business value and cost of maintenance.
- Any REB ICT asset that has been retired must be erased of any data, information and software by partitioning the relevant hard drives.
- On retirement of well-functioning or refurbished ICT assets, the relevant REB organ could decide to donate the asset to support schools. In this case, it must be

ensured that the ICT assets have been erased of any data, information and software by partitioning the relevant hard drives, before leaving REB premises.

- The senior management will propose the action to be taken regarding e-waste management.

4.9 Access control and user account management

- Access controls will be established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented;
- Logical access controls will be implemented in accordance with the information security procedures.
- Physical access controls will be implemented in line with this policy and the Physical and Environmental Security procedures;
- Access to the network, information systems and servers will be achieved by the use individual user accounts (UIDS) that will require an appropriate authentication method;
- Access to information systems and facilities will be governed by a formally defined authorization process covering the creation, modification/maintenance, re-enabling and deletion of accounts;
- Users will only be granted access to information and information systems and facilities on a "need-to-know" basis. Users will only be granted the minimum access and privileges required to perform their duties;
- Procedures will be implemented to ensure that access to data or information is not dependent on any one individual. Privileges granted by groups will be implemented in order to facilitate this function;
- Each assigned account will uniquely identify the user. Accounts must not give any indication of the user's access rights;
- Security of systems administration accounts and passwords will be the responsibility of the technical owner of that system and must adhere to REB policies with the exception of where this is not technically possible;
- A notice warning users about accessing information without authorization will be displayed before users can gain access to any information system or facility.
- User accounts will be reviewed on a regular basis to ensure access and account privileges remain applicable to the job function/role or employment status of the user. A record of the review must be maintained;
- All employees have a legal duty to keep all personal data confidential and to comply with the data protection provisions contained within the Code of Conduct for Employees;

- Access to information systems and facilities will be revoked for users who do not need access to perform their duties in order to ensure the confidentiality, integrity and availability of information to other users.
- All accounts created or modified must have a documented request and the appropriate authorization. A record must be maintained of all authorizations including the access rights and privileges granted;
- Generic or shared accounts will not be permitted without granted approval from ICT unit.
- Upon notification of termination, transfer, resignation, suspension or retirement from employment received from the relevant authoritative source(s) the user account will be disabled/ deactivated.
- Each user account must be unique, only connected with the user to whom it was originally assigned.
- All user accounts will force the use of a password as a minimum;
- All accounts must have a password expiration period.
- All connections to the Internet or other public networks must be protected by firewalls configured to filter traffic and ensure against denial of service attacks and unauthorized access to internal resources.

4.10 Password Usage and Management

- Individuals are personally responsible for maintaining the secrecy of their passwords and for controlling access to their user accounts through password security.
- It is the responsibility of systems administrators to ensure that only hashed/encoded forms of password are stored in their respective systems.
- REB will not necessarily configure its systems to enforce password complexity but users are required to choose strong passwords in order to protect their 'electronic identity', prevent unauthorized access to systems and preserve the availability and integrity of data.
- REB will not implement password aging, except in respect of those passwords that provide access to certain sensitive applications. However, where password aging is enforced for sensitive applications, system-forced changes will occur at least every 60 days.
- System administrators and computer support staff who configure new systems and set up services are to ensure that all password settings are changed from their default settings before moving platforms into production.
- All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis. However, wherever possible, changes should be implemented monthly.
- It is recommended that user passwords are changed at least every three months. They must be changed immediately on any occasion that a user believes that someone else may be aware of their password and on all occasions when a malpractice incident is discovered or suspected.

4.11 Physical and Environmental security

Computers and Server rooms:

- Access to computer and servers should be controlled and restricted to authorized personnel who need access to perform their duties.
- Use of authentication mechanisms (biometrics, swipe card plus PIN number, proximity cards) should be considered for rooms housing critical information system facilities.
- Computers and server rooms should be equipped with doors, which are resistant to forcible entry.
- Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Access rights to secure areas must be reviewed and updated every 6 months, and revoked when necessary
- Access to the server room must be restricted on a need-to-use basis. Any other person entering the room must sign the Server Room Access Log giving details like name, time in, time out, reason for entry, accompanied by, date, etc. This includes ICT staff, visitors and contractors like the maintenance team from suppliers.
- When contractors are on site, testing the network or installing new equipment, they must not be left unattended in the server room.
- Server rooms or equipment rooms containing systems classified as CRITICAL must be provided with a CCTV recording camera outside and inside the door(s) and on other principal perimeter positions to monitor and record access
- Log books of access to server rooms and equipment rooms and records from access control systems must be kept secure and archived for six months.
- Staff, agents or third-parties working outside normal business hours in server room or equipment rooms must physically sign an entry logbook maintained by site guarding staff and display their credentials for access, such as access pass, written approval, **etc.**

Visitors and Third Parties:

- Visitors and third parties should be only allowed entry to computer and server rooms for authorized and specific purposes only.
- Visitors and third parties should not be permitted unsupervised access to computer and communication rooms. This arrangement should exclude employees of outsourcing agencies who are responsible for owning or operating an information processing facility.
- The date and time of entry and departure of visitors and third parties and the purpose of visit should be recorded in a visitor's log.
- The date and time of entry and departure and the purpose of entry of authorized personnel (including employees of outsourcing agencies) outside normal business hours or assigned hours of work should be recorded in a log.
- All authorized personnel and visitors should be required to wear some form of visible identification (e.g. employee identification badges, visitor badges) within computer and Server rooms.

Information Storage Media:

- All information storage media (e.g. hard disks, magnetic tapes and CD-ROMs) containing sensitive or confidential data should be physically secured, when not in use.
- Physical access to magnetic tape, disk and documentation should be restricted to authorized personnel based on job responsibilities.
- Back-up media should be stored in fire resistant safes or cabinets
- Any personal information storage media like cartridge tapes, DAT drives and flash disks should not be allowed inside computer and Server rooms.
- Any institutional storage media (flash drives, CDs, DAT tapes) should not be allowed out of REB premises without clearance from relevant ICT manager.

Offsite Facilities:

- Fall back equipment and back-up media should be stored at a safe distance (e.g. an offsite location) to avoid damage from a disaster at the main site.
- The physical and environmental safeguards available at the off-site location should provide the same level of security, at a minimum, as at the primary site.

Cabling security:

- Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage. Controls must be carried out by entitled persons
- Network cabling must be swept for unauthorized attached devices at least once every 3 months.
- Access to network or power cabling, junction boxes, communications equipment and service ducts in general REB premises must be physically restricted
- Data centers must be provided with at least two independently routed trunk communications links to carrier networks to avoid a single point of failure in communications
- Network cabling shall be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas.
- Power cables should be segregated from communications cables to prevent interference.

4.12 Information Classification

- All information in Government is classified to indicate the need, priorities and expected degree of protection that should be ensured while handling the information.

  The Classification Categories are:

  - Strictly Confidential

- Confidential
- Internal
- Public

➢ It is the responsibility of the asset owner to define the Classification of the asset, periodically review it, and ensure it is kept up-to-date and at appropriate level.

➢ The asset owner may also specify the access rights / approve authorization of user to access the asset.

➢ It is responsibility of the information users to ensure compliance to the defined categories.

➢ The detailed information classification is referred to Asset Management Policy.

4.13 Backup and Disaster Recovery

- REB's data will be stored and retained on network drives unless other suitable backup arrangements have been determined and approved by ICT Unit
- Data will not be removed from network drives unless it has been determined that this data will not be required in the future.
- Data will not be stored on local PC drives unless it is fully backed up to a suitable network location.
- ICT Unit will develop and document appropriate backup strategies to ensure important data is protected against loss.
- An ICT backup and disaster recovery plan (ICT BDR plan) must be established, maintained and periodically tested for all critical information resources.
- The ICT BDR plan must define:

  ✓ Procedures for assessing damage, escalation and disaster declaration.

  ✓ Roles and responsibilities of disaster recovery team members, including third parties, their contact details and communication procedures.

  ✓ Prioritised recovery procedures based on critical information resources.

  ✓ Backup procedures, manual procedures, alternative processing facilities and safety and health procedures.

- The ICT BDR plan must be stored in hard and soft copy in a place of safe storage and must be accessible in the event of network failure.
- The ICT BDR plan must be securely distributed and available only to authorised personnel.
- Key backup devices must be stored and easily accessible in the event of a disaster.
- Disaster recovery training sessions must be conducted to ensure preparedness for a disaster.

- Backups must be performed based on a defined cycle and must include, at a minimum critical databases' master files and transaction files, critical applications, configuration settings and user documentation.
- Backup media must be clearly labelled, prevented from overwriting, appropriately stored and protected in transit e.g. in secure containers.
- Backups must be checked periodically to determine whether recovery is possible.

4.14 Email and internet

- Personal Emails are not permitted to be used for REB related activities, only REB Emails are allowed.
- Individuals must not send, forward or receive confidential or sensitive REB information through non-REB email accounts.
- REB Email should not be used for conducting personal businesses.
- Broadcasting Email to all staff is prohibited except when approved and authorized by ICT Manager.
- All email accounts maintained on REB email systems are property of REB, Passwords should not be given to other people and should be changed frequently. Email accounts not used for 30 days will be deactivated and possibly deleted.
- All files downloaded from the Internet must be scanned for viruses using the current virus detection software
- REB may monitor and log the use of its network whenever there is a well-founded suspicion that illegal, prohibited or wrongful conduct is taking place for the purpose of verifying compliance with this policy and guaranteeing the integrity and security.
- Access to the Internet will be provided to users to support REB activities and only when needed to perform their jobs and professional roles.
- A limited access to REB network is allowed to interns and other visitors for security purpose.

5. Responsibility

- The Directorate General shall have oversight responsibility for the internal ICT policy implementation, monitoring and evaluation.
- There will be an internal ICT steering committee chaired by the head of ICT in Education and Open Distance e-Learning (ODeL) Department. It is composed of at least one member of the senior management, head of Corporate Services Division, director of ICT unit, all directors of ICT in Education & ODeL Department.
- The ICT Unit main responsibility is to operationalize REB ICT internal policy, including ICT systems, security strategy, disaster recovery plan, maintenance, ICT services, procurement, distribution and asset management.

6. Non-Compliance

REB reserves the right to audit compliance with this policy on a regular basis. Employees who break the provisions of this policy will be disciplined according to the law establishing the general statutes for public service.

7. Glossary

Disaster recovery	The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure
Backup	Refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.
e-Waste	Refers to all waste caused by discarding electronic devices, especially consumer electronics
Third-party software	Reusable software component developed to be either freely distributed or sold by an entity other than the original vendor of the development platform
ICT environment	ICT environment refers to all the computers, servers, monitors, printers, cables, routers, switches, software, data, information systems, internet connectivity, emailing, scanners, modems, mouse, keyboards, laptops, UPSs, data backups, antivirus protection, hardware repairs, internet usage, user log-on, security permissions, web sites and telephones.
Change control	Process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner.
Counterfeit software	It is the illegal software obtained by re-copying or re-manufacturing the legal software products without any authorization from the original vendor.

8. Authorisation, Approval, Review and Amendment Sheet

8.1 Approval and Amendments Sheet

This policy is authorised by:

Dr John Rutayisire
Director General

_____
Signed

_____
Date

This policy has been endorsed and signed off by the members of the senior management:

Dr. Evode Mukama
HoD, ICT in Education and ODeL

Signed _____

Date _____

Dr. Joyce Musabe
HoD, CPMD

Signed _____

Date _____

Mr. Janvier Gasana
HoD, EQSD

Signed _____

Date _____

Mr. Emmanuel Muvunyi
HoD, EAD

Signed _____

Date _____

Mrs Louise Karamage
HoD, HESLD

Signed _____

Date _____

Mr Nkubito Bakuramutsa ***Signed*** _____
Coordinator, OLPC

Date _____

Mr Peter Njishi Mujiji ***Signed*** _____
HoD, CSD

Date _____

8.2 Review

In order to ensure that REB ICT assets are adequately protected and that this policy remains relevant, this policy will be reviewed every year and when deemed necessary.

8.3 Records of Amendments

Version no.	Description of Amendment	Date