REPUBLIC OF RWANDA

RWANDA EDUCATION BOARD (REB)

REB HEADQUARTERS BUILDING

VOLUME IX: PROCEDURES MANUAL

FOR

ICT SUPPORT UNIT

This procedures manual for ICT support Unit is Volume IX of the REB comprehensive manual. Volumes within this series are:

VOLUME	DEPARTMENT/UNIT
CORE DEPARTMENTS	
I	Curriculum Pedagogical Materials Production and Distribution (CPMD) Department
II	Education Quality and Standards (EQS) Department
III	Teacher Development and Management (TDM)
IV	Examinations and Accreditation (EA) Department
V	ICT in Education and Open Distance and E-Learning (ICTE& ODEL) Department
VI	Higher Education Student Loans (HESL) Department
SUPPORT DEPARTMENTS/UNITS	
VII	Corporate Services Division
VIII	Planning & Research
IX	ICT support Unit

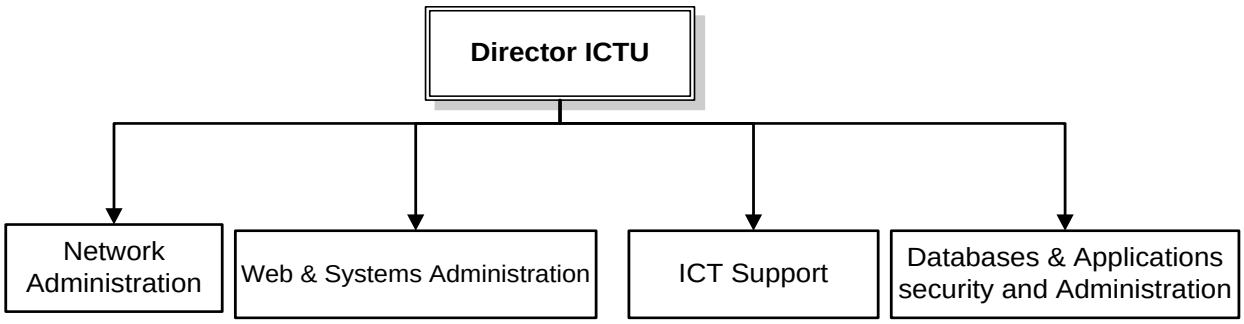
TABLE OF CONTENTS

9.0 INTRODUCTION

The ICT Unit has developed ICT policies designed to serve as a framework for the elaboration, management and utilization of REB ICT systems. The procedures outlined here and their attendant rules and regulations, should guide REB staff at all levels to acquire, use and develop ICT culture in their daily activities.

The REB-ICT environment includes all computers, servers, monitors, printers, cables, routers, switches, software, data, information systems, internet connectivity, emailing, scanners, modems, mousse, keyboards, laptops, UPSs, data backups, antivirus protection, hardware repairs, internet usage, user log-ons, security permissions, web sites and telephony.

9.1 MICRO STRUCTURE



9.2 FUNCTIONAL RESPONSIBILITIES

The unit has the following functional responsibilities:

- Develop and implement policies and procedures for electronic data processing and computer systems operations and development;
- Design, develop, implement, operate and administer computer and telecommunications software, networks and information systems;
- Provide the day to day technical support within REB departments;
- Control the unit budgets and expenditures;
- Ensure technology is accessible and equipped with current hardware and software;
- Provide individual training and support on request;
- Provide recommendations about accessing information and support;
- Maintain current and accurate inventory of technology hardware, software and resources;
- Maintain log and/or list of required repairs and maintenance
- Monitor and maintain the use of the photocopiers and printers.

9.3 ICT CORE PROCESS ACTIVITIES

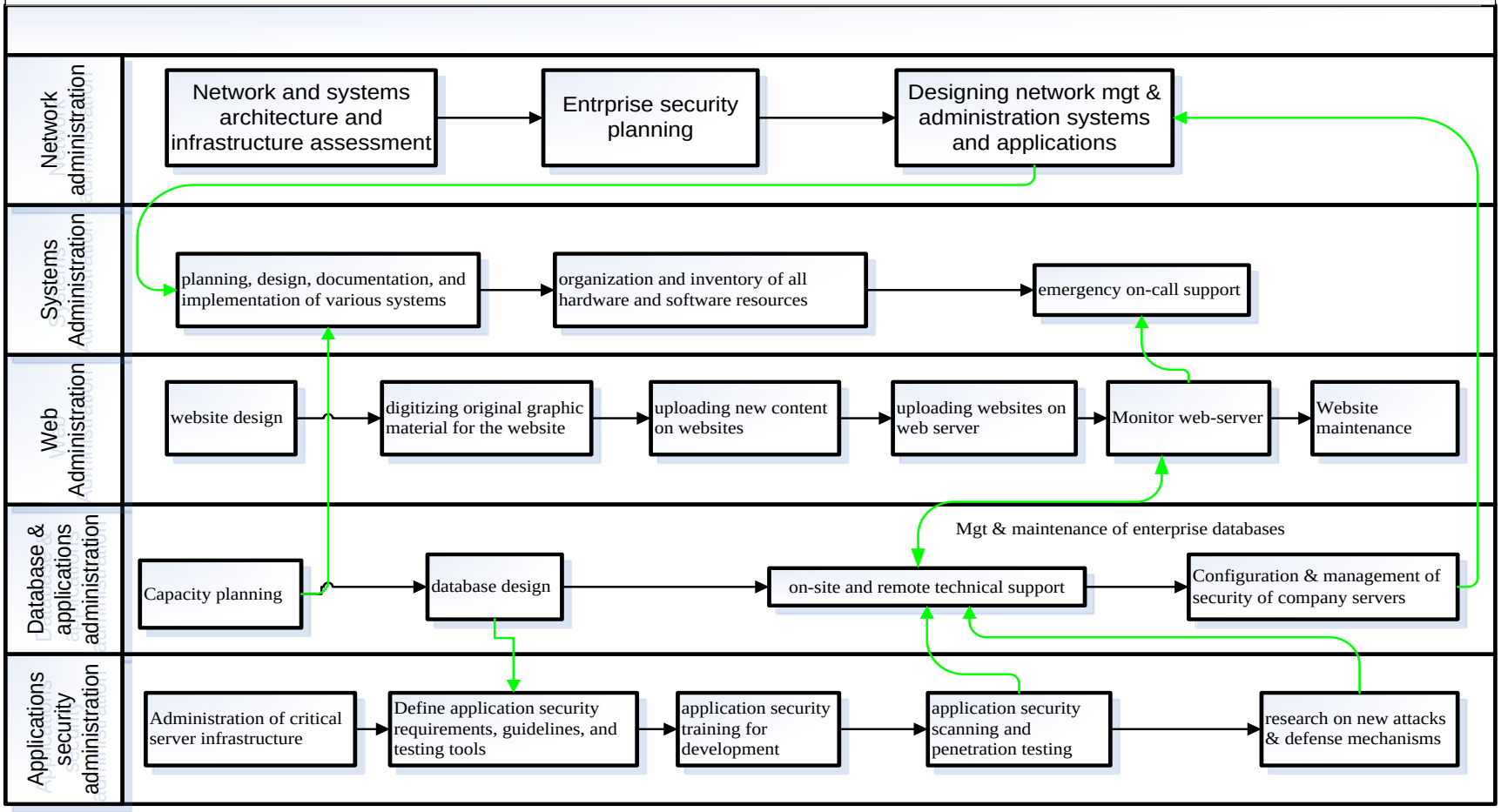
The following core processes underlie the processes and activities across the different sections of the ICT Unit:

- REB ICT infrastructure project development and management
- ICT support (software and hardware acquisition, use and maintenance)
- Web development, management and maintenance
- ICT security

9.3.1 PROCESS MAP

A process map depicting the above core processes across the sub units is provided in the process flow map overleaf.

Processes flow map for ICT Unit



The procedures to guide the efficient and effective management and utilization of REB ICT systems are provided for the following processes:

- REB ICT infrastructure project development and management
    - ICT project management
    - Change management
- Software and hardware acquisition, use and maintenance
    - Hardware acquisition, use, maintenance, replacement and storage
    - Software acquisition
- ICT support and maintenance
    - Access control and user management
    - Password usage
    - ICT systems support and maintenance
- ICT security
    - Physical and environmental security
    - Security monitoring
    - Back up
    - Anti-virus protection

9.4 RULES, REGULATIONS AND PROCEDURES FOR CPMD DEPARTMENT

FUNCTIONAL PROCESS	POLICY	PROCEDURES
REB ICT Infrastructure project development and management	Policy: ICT project management	• The user/beneficiary departments will identify the business need / requirement that need to be fulfilled. • Design and define high level solution that provides a solution to the business requirement. This will clearly identify business goals, scope, requirements and deliverables. • The Project Initiator shall develop a Project Initiation Document which will be approved by the ICT director together with the Head of the User/Beneficiary department. A Project Manager will be identified and appointed. • The Project Manager will develop a project implementation activity schedule, with resource and related costs. This will be approved by the Project Sponsor represented by the ICT director and Head of User department. • The Project Manager will ensure the project is implemented according to schedule, budget and desired quality/set of deliverables. Any changes will first be approved through a formal change management procedure. • Once all activities have been performed, the Project manager will test for completeness and document • The project manager will then handover and close the project.

FUNCTIONAL PROCESS	POLICY	PROCEDURES
	Policy: Change management	The primary goal of the IT change management organization is to accomplish IT changes in the most efficient manner while minimizing the business impact, costs, and risks. To achieve this, the change management process includes the following primary steps: • Formally Request a Change. All requests for change will be documented within REB's selected technology platform by creating a new change record. The completion of a new request for change will be completed by the ICT Director with input from the Change Requester. • Categorize and Prioritize the Change. The ICT Unit Director or other designated IT will assess the urgency and the impact of the change on the infrastructure, end user productivity, and budget. • Analyse and Justify the Change. The ICT unit staff works with the change requester and the change initiator to develop specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. IT staff use this information to further research and develop an extensive risk and impact analysis. When completing the analysis of the change, the IT staff must ensure they consider the business as well as the technical impacts and risks. • Approve and Schedule the Change. The IT staff uses the REB's selected technology platform to record an efficient process for routing the Request for Change (RFC) to the Change Coordinator, technical approvers, and business approvers and, in the event of a major or significant change, to the Change Advisory Board (CAB) for approval or rejection of the change. • Plan and Complete the Implementation of the Change. This process includes developing the technical requirements, reviewing the specific implementation steps and then completing the change in a manner that will minimize impact on the infrastructure and end users. • Post-Implementation Review. A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success; and finalizing the change documentation within REB's selected technology platform.

FUNCTIONAL PROCESS	POLICY	PROCEDURES
Software and hardware acquisition, use and maintenance	Policy: Hardware	**Ownership and asset registration** • All purchased IT equipment must be registered by ICT Unit with logistic unit before first use. • The Head of ICT will be responsible to forward to the Finance a list indicating type of IT equipment, the owner of the equipment and depreciation time for that equipment. **Usage** • Upon receipt of new IT equipment, user signs Equipment Reception Form. • Transfer/borrowing of IT equipment must be ensured by IT Technician and the user will be responsible for data and safety of equipment on return. • When the user leaves the employment, he/she must hand over all hardware to the Director of Unit or to the IT Unit. **Installation** All installation and configuration of REB IT equipment covered by this policy is the responsibility of ICT unit staff. **Taking equipment off site** • Any request to take IT equipment out of the office must be approved by Head of Department and IT Director. • All equipment taken out have to be registered and the same on return. **Personal equipment** • Personal equipment not allowed to be used on REB network, unless it is requested by the user and approved by ICT Director. • The owner of the equipment is responsible to get permission before use. **Replacement of equipment** • IT technicians will periodically or according to the status of equipment and based on equipment depreciation time get a list of old, corrupted, or unnecessary equipment in all REB department for storage. • ICT Unit together with Finance and Logistic unit will propose the action to be taken regarding the stored equipment which are no longer possible to be repaired or unnecessary or which has passed depreciation time and can cause security risk. **Maintenance** • Only the system administrator has the right to add a computer to the corporation domain • All hardware problems have to be reported to ICT Unit and registered in ICT complaints database. • Supporting REB staff/users is to be performed by IT staff or contracted external company.

FUNCTIONAL PROCESS	POLICY	PROCEDURES
	Policy: Software acquisition	The following are procedures for acquisition of software: a. User department will present the business use for the new software b. Request study or case validation c. He request can be accepted and approved by Director of ICT or rejected and sent back to the user for more information. d. If approved, ICT team shall see whether REB has the capacity to develop the software. If not, the acquired software will go to tender from external vendors. e. If software is developed internally, the software will be tested by the user department and approved by user department and ICT unit. f. If the software does not meet user requirement it shall be reverted back to development for further customization or developed g. The software shall be licensed and handed over to the user for usage.
ICT support and maintenance	Policy: Access control and user accountant management	• Conducting background and security checks of users requesting access to REB applications are and remain the sole responsibility of REB ICT Unit. • Users must request access to the system through the use of a User Requisition template. • User Help Desk (UHD) will approve the user's access and determine the user's appropriate level of access or role in accessing the requested application. Where appropriate, UHD will verify with the party responsible for authorizing the user's access. UHD will provide the user with a user name and a password. The password is set to expire upon initial user log in and must be re-established following the password rules established in the password policy guidelines. • Where appropriate, training on the application must be completed prior to being granted access. • It remains the sole responsibility of the user's department to inform UHD when a current user's access must be revoked, limited or modified because of security issues, transfer of personnel, change in employment role or responsibility, separation or employment, or employment status change (i.e., change of employee function hence access no longer required). • All appropriate REB sites will use this procedure for guidance relative to establishing user accounts to REB applications and information systems.

FUNCTIONAL PROCESS	POLICY	PROCEDURES
	Policy: Password usage and management	• Users should be required to sign an undertaking to keep personal passwords confidential. This signed statement could also be included in the terms and conditions of employment. If users are required to maintain their own passwords, they should be provided with a secure initial password, which they should be required to change immediately at first logon. • Procedures should be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password. • A secure procedure should be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages should be avoided. • Temporary passwords should be unique and should conform to password standards. • Users should acknowledge receipt of passwords. • Passwords should never be stored on computer systems in an unprotected form. • Default vendor passwords should be replaced as soon as the installation of systems or software has been completed
	Policy: ICT Systems support and maintenance	- Each request should be recorded using ICT complaints database - The maintenance and request form to be filled by the user should have the following information: ✓ Name of User / Department ✓ Type of requested support ✓ Brief description of problem - Support request should be processed and record the status - External Maintenance or Support: for external support, request will be revised by ICT Team and forward the suggested way forward to the finance for approval - The support person will then review the situation, visiting the user if need be. On completion, the following is entered on the request form: ✓ Time/Date started processing the request ✓ Time/Date completed processing the request ✓ Real problem: as the user may have phrased the problem wrongly, the support person will enter the actual cause or issue of support. ✓ Action taken: describes what was done to solve the problem or give support

FUNCTIONAL PROCESS	POLICY	PROCEDURES
ICT security	Policy: Physical and environmental security	Server room access procedure: • The employee or visitor's sponsor submits signed request for access to server room by completing a server room access control form stating the reason, duration and proposed timing of the visit. • Server room access control form is approved by the Director ICT. • Director ICT assigns the system administrator or designate employee who is the custodian of the server room to grant access to the server room. • The system administrator or authorized staff with access rights to the server room escorts the staff or visitor to the server room. • Both the system administrator, escort and the visitor/escorted persons sign the data server room access log book indicating time, date and reason for entry. • The system administrator or designate must be present at all times when the visitor is in the server room. • Once the purpose for the visit has been accomplished, the staff/visitor will sign out of the visitors log book. • Exit the server room Access Procedure for Staff members to ICT premises: • When entering REB ICT premises, all staff members should clearly display their identification cards. • The staff member places his/her luggage including all metallic items in his/her possession onto the tray/table next to the metal detector and walks through the detector. • If the employee doesn't activate the metal detector, his/her luggage is searched to ensure that harmful items aren't being brought in illegally. • If the search produces nothing of importance, allow the employee to proceed. • If a harmful item is found in the employee's possession(s), the employee is handed over to the security guards for interrogation into the matter. • If the employee activates the metal detector, he/she is asked to put any other metallic objects on him/her on to the tray/table next to the metal detector and after the removal of such objects, the employee walks through the metal detector a second time. • If the metal detector is activated again, request the person to submit himself/herself to a physical search. • If the employee is willing to be searched, a guard passes the hand-held metal detector over the clothes/body of the employee. • If anything suspect is detected, the staff shows the object to the guard. • If the staff refuses to show the suspect object to the guard, he/she should be escorted off REB premises. • If it is a harmful object, the employee is detained by the security guard while the security team is informed. • The employee is handed over to the security team or ICT director so that disciplinary action can be taken. • If the search produces nothing of importance, the employee's luggage is searched to ensure that harmful items aren't being brought in illegally. • If the employee refuses to submit to a search, draw his/her attention to the search procedure and security policy and inform him/her that he/she can't access REB ICT premises unless he/she is checked thoroughly. • If the employee still refuses to be searched, inform the security team so that the situation can be resolved.

FUNCTIONAL PROCESS	POLICY	PROCEDURES
	Policy: Security monitoring	I. Logging procedure Daily basis: The IT Director will liaise with the Heads of Department or system owner to set up the respective system to log the following security events on a daily basis: a. All security violations, such as System access denied, Invalid password, Invalid security certificate, Password revoked, and Resource access denied b. All accesses to sensitive/significant areas of the systems. c. All security commands issued using the security administrative authority. d. All accesses to operating system resources, with the exception of the default access. If the resources can be read publicly, record the update or allocation and deletion of access e. Successful connections; f. Denied connections and rejected attempts g. Failed attempts to access files, resources and other object; h. Successful attempts to access REB information; i. Logon successes and failures; j. Error messages and alerts; k. Lengthy connection times; l. Duplicate user names and concurrent user sign-on; m. Account creation and maintenance; n. Firewall activity; II. The identity of the user, or processes activated by the user, must be maintained for the duration of the sessionThe following information must be logged for each security-related event that occurs within each application or infrastructure environment: i. Event type/description (e.g. unauthorized logon); ii. Process or user identifier associated with event; iii. Workstation/terminal identifier and network address associated with event; iv. Files or objects affected by event v. Date and time of event; vi. Identifier of platform and application recording the event. III. The following changes to users' access control and rights that may occur within each application or infrastructure environment must be logged: i. Creation of a user profile; ii. Deletion of a user profile; iii. Renaming of a user profile; iv. Modification of user profile access rights; v. Change to user profile password characteristics. IV. The following must be logged as evidence of unauthorized or unusual use: i. Successful login and logout; ii. Unsuccessful login; iv. Failed attempt to access controlled files, directories or other resources; v. Unauthorized access controlled files, directories or other resources. vi. Changes of user passwords must be logged. V. The following changes to the operation or content of the security audit log that may occur

FUNCTIONAL PROCESS	POLICY	PROCEDURES
	Policy: Backup	a) The following are guidelines of procedures and responsibilities for ICT staff. These guidelines will include backup strategy that applies to the following: • Computerized systems that store REB information • Implement backup for each type of computer system in use. b) Backups should occur on a daily basis or be based on the significance of the information and its frequency of change. A preferred method of backup is disk-to disk backup. If this method is not applicable for the system, then tape backup is required. c) Back up all necessary data files and programs to recreate the operating environment. d) Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location. An inventory and tracking system must be maintained. Ensure that the following are stored at the off-site storage location: • Source and object code for REB programs • Master files and transaction files necessary to recreate the current master files - System and program documentation - Operating systems, utilities, and other environmental software - Other necessary records e) Ensure that documented procedures exist for the recovery and restoration of information from backup media. f) Identify I.T. staff responsible for ensuring successful back-ups. g) Routinely copy operating software, application software to backup media based on frequencies set by management. This applies to major systems (e.g., local area network (LAN) or wide area network (WAN) servers, client/server database servers, special-purpose computers) in use by departments. h) Maintain at least three generations of backup media, i.e. "grandmother, mother, daughter" arrangement for operating and application software. i) Define data model to be used for each type of data; i.e. full + incremental, full +differential, (for file servers) or database exports or extracts (for applications). j) Back up of the printed documentation and pre-printed forms necessary for recovery. Convert printed documentation and pre-printed forms into electronic format and move them into the DR site. k) Test the backup to determine if data files and programs can be recovered.
	Policy: Anti-Virus protection	Procure antivirus using standard procedures Provide specifications from IT Technician The company that provided the antivirus together with ICT staff install the anti-virus The installation includes updating. Thereafter REB ICT Unit staff regularly advises the user on how to continuously update. Any other help is handled following ICT support guidelines described above.