MINEDUC Internal ICT Management Policy

TABLE OF CONTENTS

1. Introduction and Methodology

In order to improve the value that ICT delivers to the Ministry of Education, an ICT strategy has been developed which seeks to forge closer working relationships, build trust and set a common purpose for ICT throughout the Ministry. This strategy aims to bring the various elements of ICT together and ensure that the ICT discipline works towards achieving a common, relevant and shared vision with the business. A policy defining the minimum acceptable ICT management practices is necessary to facilitate the implementation of the agreed IT strategy.

This policy document has been developed using the following methodology:

i. The need to develop an internal ICT Policy was determined by the Management of the Ministry of Education, in order to ensure that the use of ICT within the Ministry of Education is managed in a controlled fashion according to the needs of the Ministry.
ii. The initial draft was formulated following a review of international standards in the management of ICT within organisations and also taking into consideration the Government of Rwanda policies related to the use of ICT within government organisation.
iii. A stakeholder consultation was undertaken with all the main stakeholders of the users of ICT within the Ministry of Education on 3rd December 2012.12.03
iv. The comments from the Stakeholder consultation have been incorporated in this final draft which is being circulated around stakeholders for their final comments.
v. The target for final approval of the document is 12th February 2013.
vi. Following final approval the policy will move to implementation stage with the first task to raise awareness among the users of ICT within the Ministry and the staff who will be required to oversee the implementation of this policy.

2. Scope

This policy applies to all the ICT Functions of MINEDUC, hereinafter referred to as the ICT discipline and is issued by the MINEDUC Management Team, to be managed by the Information and Communication Technology discipline of the Ministry of Education. This policy applies to all ICT equipment installed within the Ministry of Education only. ICT installed in agencies of the Ministry and in schools and other learning institutions are covered under separate policies such as the broader ICT in Education Policy and individual Agency ICT policies.

3. Objective

The objective of this policy is to clearly define the processes and procedures to ensure the effective management and implementation of all ICT services to meet the requirements of the Ministry of Education within a performance measurement framework. The objective is:

- To enable the monitoring and improvement of service quality through the effective application of processes.
- To ensure ICT activities are aligned with the Ministry needs and objectives.
- To improve the utilisation of resources.
- To provide services that meet the Ministry's business, stakeholder and user needs.
- To improve the quality of project deliverables and timescales.
- To improve risk management and resilience.
- To ensure that staff are fully aware of their roles and responsibilities and developed to perform their roles effectively.
- To ensure compliance with all corporate standards relating to the implementation of IT Service Management practices as mandated by the Government of Rwanda

4. Policy Statement

4.1 General

- This policy has been developed utilizing the CobiT framework. CobiT has been identified as the ICT Governance framework of choice to many ICT Professionals. By incorporating the CobiT methodology into our business processes, we will be able to achieve a high level of confidence in the integrity of our core activities.
- Although the ICT strategy articulates a clear demarcation of accountability and responsibility, all MINEDUC ICT professionals are jointly and severally accountable for successful delivery to the business.

4.2 Planning

- ICT strategic planning process must be established and maintained. An assessment of the ICT Strategy must occur in the first quarter of every year to ensure that the strategy evolves with technological change. The strategy must also be revisited for relevance in response to significant business change.
- ICT balanced scorecard (BSC) must be established and maintained to ensure the successful implementation of the MINEDUC ICT strategy. The MINEDUC ICT BSC must have clear linkage to the strategy, and the BSC must cascade to individual Key Performance Indicators.
- A clearly defined enterprise architectural framework must be established and maintained to ensure common ICT standards, and optimise the management of ICT across all levels of the Ministry's organisation.

- ICT standards must be agreed upon in collaboration with key stakeholders(RDB/IT). The ICT discipline must adhere to the agreed ICT standards and ensure compliance within their respective business units.
- ICT standards must be continually evolved and revisions communicated.
- All ICT purchases must comply with the agreed national standards as defined by RDB IT and RBS, and where no standard exists for a given technology; the request must be submitted to the ICT office for ratification and, if successful, incorporated into the ICT standards.

4.3 Project Management

- All major ICT projects, must follow a formal project management methodology. This methodology must, at a minimum, stipulate the following project deliverables within the respective phases of the project:
  - Project Initiation – Project charter.
  - Project Definition – Project definition report, Project plan and Business justification.
  - Execution – Project status reports.
  - Close out – Project completion report
  - Maintenance

4.4 Risk Management

- A risk management process must be followed that is aligned to the RDB/IT Risk Management Guidelines.
- A risk log must be maintained for the most significant ICT risk issues identified and these issues must be followed up regularly.
- An annual audit certificate must be issued by all ICT functions within the ICT discipline.

4.5 Information Retention and Disposal

- Information must be retained and disposed of in line with statutory and business requirements. Failure to comply with statutory and business requirements could result in a financial loss, legal action, and embarrassment to MINEDUC, unavailability of information and wastage of resources in managing obsolete information.
- Identify, for each information resource that should be retained, the most cost-effective means of retention.
- Store information on storage media that is the most cost-effective and meets statutory requirements.
- Ensure that when highly confidential and restricted information is destroyed, its confidentiality is not compromised.
- Ensure that information that is classified as Highly Confidential or Restricted has appropriate levels of access control.

- Index all information stored in a repository to facilitate easy identification, retrieval, and destruction at the end of its retention period.
- Destroy information that falls outside of retention periods specified by business or that is obsolete and no longer has any value to the business.

4.6 ICT Asset Disposal

- In order to prevent the deterioration in the productivity of MINEDUC 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	3 years
Printers, Scanners, Modems	3 years
Servers, mini or mid range computers	3 years
Desktop software, operating systems	3 years

- It must be noted that these are the minimum terms and that each decision to retire an IT asset must be viewed in terms of the residual business value and cost of maintenance.
- Any MINEDUC ICT Asset that has been retired must be erased of any data, information and software by partitioning the relevant hard drives.
- On retirement of an IT asset, in consultation with the Ministry of Infrastructure ,the relevant ICT function could decide to donate the asset to support Schools after they are refurbished. In these cases, 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 MINEDUC premises.

4.7 Acquisition

- Before ICT solutions are investigated, there must be a valid business requirement with a formal definition of information requirements that is agreed between the user and ICT office and auditable.
- All IT purchases must be conducted in accordance with GoR' Procurement policies and procedures.
- In the absence of preferred suppliers for a specific service, alternative courses of action must be investigated, as part of a formal RFP process and scored on a number of qualitative and quantitative criteria that will determine the suitability of a given IT solution. This process must be conducted in an auditable fashion.
- A technological feasibility study must be conducted to ensure that the proposed ICT solutions will be compatible with the ICT architecture. ICT security and risk considerations must be built into the ICT architectural criteria. The enterprise

architecture office must be consulted to ratify whether there is an appropriate technical fit.

- An economic feasibility study entailing a cost-benefit analysis must be conducted to establish the availability of sufficient funds to implement the preferred alternative solution.
- An audit trail design must be documented to indicate what events require logging, what data should be logged, how sensitive data in logs are to be protected, who should review the logs, the frequency of the review and the retention period. Audit trails or log files must be protected from unauthorised access and their distribution must be in line with their security classification.
- Ergonomic factors must be taken into consideration and must be in line with regulatory requirements.
- When selecting ICT solutions, the software licensing requirements must always be adhered to, to ensure that MINEDUC is in no way exposed to liability in terms of illegal 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.
- A formal report, taking the considerations mentioned above, must be compiled detailing the selection of an appropriate vendor.
- In the case of new or modified computing facilities, a formal acceptance of facilities must be signed by the MINEDUC appointed project manager, stating that the facilities are in compliance with local and national regulations.

4.8 Applications Development

- All applications development must follow a defined software development lifecycle (SDLC) that at a minimum:
  - Translates business requirements into detailed design specifications that includes:
    - Input requirements definition and documentation
    - Interface definition
    - Source data collection design
    - Program specification
    - File requirements definition and documentation
    - Processing requirements
    - Output requirements definition
    - Internal controls
    - Auditability
    - Security and availability
    - Testing requirements

- Ensures that, as part of any new applications development, new hardware and software are assessed for their impact to the ICT environment before deployment and considers performance, capacity planning, and tuning, integration and security requirements upfront.
- Establishes user procedures manuals, operations manual and training materials as part of any new applications development.
- Defines an implementation plan encompassing roll-out/installation procedures, incident handling, distribution controls, storage of software, as well handover from development to testing to production.
- Specifies a test plan based on the enterprise architecture and defines roles, responsibilities and success criteria including final acceptance criteria.

4.9 Software Licensing

- Only software for which a legal contract exists may be installed onto MINEDUC ICT assets by the IT Professionals.
- 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 MINEDUC premises or elsewhere unless MINEDUC' is expressly authorised to do so by agreement with the licensor, and this has been approved by the relevant ICT manager.
- Software e.g. CD's may not be loaned to any users or contractors unless expressly authorised to do so by agreement with the licensor, and this has been approved by the relevant ICT manager.
- Software on multiple machines may only be installed in accordance with the applicable license agreements.
- A register of software and the software licensing details must be maintained and updated on a regular basis.
- No Shareware or Freeware may be loaded onto MINEDUC ICT assets without the written permission of the relevant ICT manager.

4.10 Provisioning of ICT services

- The service level management framework must include the establishment of a service catalogue, service descriptions and comprehensive and measurable service level agreements.
- Performance against agreed service levels must be regularly reported on and service improvement programmes implemented to address service level deviations.
- A regular review of service level agreements and underpinning contracts with internal and external service providers must occur to ensure that they are effective, up to date, and changes in requirements have been accounted for.

- A detailed chargeback model, clearly articulating the value and cost for each service, must be linked to the service levels and regularly reviewed to ensure rates and services remain appropriate and in line with industry norms.
- A service desk function must serve as a single point of contact to register, communicate, dispatch and analyse all reported incidents, service requests and information demands.
- An escalation process must be applied that ensures that calls are acted on based on their agreed service levels.

4.11 Change Control

- All changes to the IT 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 and urgent changes must 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.

4.12 IT Asset Management

- MINEDUC ICT assets must be managed across their full lifecycle encompassing acquisition, redeployment, storage and disposal.
- An inventory of all MINEDUC ICT assets including hardware e.g. servers, workstations, laptops, PDA's, modems, switches, routers, firewalls, printers must be maintained and kept up-to-date.
- An initial baseline must be developed containing all MINEDUC ICT assets and compared regularly against a physical inventory of MINEDUC ICT assets to identify changes.

4.13 Logical Security

- Unique user identification and authentication systems must be applied to prevent unauthorised access to internal resources e.g. passwords, pins, and token devices.
- User account management must be enforced and a formal process must be followed for requesting, approving, establishing, issuing, suspending, modifying and closing user accounts.
- Access rights must be reviewed and confirmed periodically.
- Access privileges must only be granted on a need to use basis and in accordance with the relevant user's requirements necessary to carry out their job function.

- 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.
- Data encryption facilities must be utilised in accordance with the MINEDUC Information Classification Scheme contained in the MINEDUC IT User policy to prevent inappropriate access to sensitive information.

4.14 Physical Security

- Computer facilities rooms must be unobtrusive and give minimum indication of their purpose.
- The location of computer facilities rooms must be protected by sufficient physical barriers and must be sited away from areas of public access or direct approach by vehicles.
- No resources within computer facilities rooms may be visible externally.
- Wiring closets must be physically secure with only authorised access possible and the cabling routed as much as possible underground or through secured conduits.
- Doors, windows, elevators, docking stations, air vents and ducts and other methods of access to the computer facilities rooms must be adequately secured.
- An appropriate alarm system must be installed in the computer facilities rooms.
- Access to computer facilities rooms must be controlled by card readers or another adequate security system.
- Visitors to computer facilities rooms e.g. cleaning staff, third parties etc must be escorted and reasons for entry must be logged.
- **Password Use**
  - User will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical user accounts shall be maintained securely.
  - Users will change passwords whenever there is any indication of possible system or password compromise.
  - Users will change Passwords at regular intervals 90 days or based on the number of access (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid reusing or cycling old passwords.
  - Users will change temporary passwords at first logon
  - Users must not include password in any automated logon process, e.g.: stored in a macro or function key
  - Users will not share their passwords with anyone
  - Users will ensure that nobody is watching when the password is being entered
  - Wireless access points shall be secured with help of a security key

Passwords should be:

- unique
- alphanumeric
- at least 6 digits in length
- regularly changed.

Passwords should NOT be:

- written down
- easy to guess

4.15 Environmental Control

- Hazardous or flammable materials may not be stored in the computer facilities rooms or near any other critical information processing equipment.
- Eating, drinking or smoking inside the computer facilities rooms is strictly prohibited.
- Dust covers must be used to protect critical information processing equipment.
- Human friendly fire prevention and detection systems must be installed in the computer facilities rooms and must be regularly tested.
- No unsafe electrical wiring or cluttered areas are allowed within the computer facilities rooms.
- Power protection controls must be installed to prevent power outages or surges e.g. uninterrupted power supply systems, lighting conductors and back up generators.
- Air conditioning, ventilation and humidity controls must be installed and kept at optimum levels.
- Sufficient drainage must be employed in computer facilities rooms to prevent flooding.
- Safety and health measures must be implemented in computer facilities rooms e.g. clearly marked escape routes and first aid kits.

4.16 Business Continuity and Disaster Recovery

- A Business continuity and disaster recovery plan must be established, maintained and periodically tested for all critical information resources.
- The plan must define:
  - Procedures for assessing damage, escalation procedures and declaring a disaster.
  - Roles and responsibilities of disaster recovery team members, including third parties, their contact details and communication procedures.
  - Prioritised recovery procedures based on the criticality of information resources.
  - Backup procedures, manual procedures, alternative processing facilities and safety and health procedures.
- The ICT DR 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 DR plan must be securely distributed and available only to authorised personnel.
- Essential 'hot' spares must be stored and be easily retrievable in the event of a disaster.
- Reciprocal agreements must be entered into with all parties involved in the disaster recovery process.

- Disaster recovery training sessions must be conducted to ensure preparedness for a disaster.

4.17 Performance and Capacity management

- Daily health checks must be conducted on critical ICT resources. The checks must include, amongst others disk capacity, network bandwidth, buffer sizes, database size, error logs, consumables e.g. printer toner, printer paper, WAN and LAN connectivity checks.
- Performance reporting must occur on all critical IT resources on a regular basis.
- Performance requirements must be included as part of every new applications development, implementation or modification project.
- Capacity planning reviews must be conducted regularly to forecast future ICT requirements.

4.18 Data management

- Procedures must be implemented to prevent access to sensitive data and software from equipment or media when they are disposed of or used for another purpose e.g. partitioning of hard drives
- Storage and retention arrangements for data must be in accordance with legal, regulatory and business requirements.
- 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 of sensitive data must be protected in accordance with the GoR Information classification scheme e.g. encrypted when necessary.
- Backups must be checked periodically to determine whether recovery is possible.

4.19 Internal Control Assessment

- Self assessments on all ICT processes utilizing CobiT must be conducted, at a minimum, annually.
- Internal audit reviews on all ICT processes utilizing CobiT must be conducted, at a minimum, every third year.

4.20 Email Usage

The use of personal emails for work related communication is strictly prohibited. MINEDUC staff are allowed to only use MINEDUC email for official communication.

- Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.
- Users shall comply with GOR's e-mail policy on proper and effective use of e-mail.

- Users shall archive his/her emails on regular intervals. Users should protect their email account on the server through strong password and should not share their password or account with anyone else. All such locally stored emails on critical laptops/ desktops shall be protected by a password.
- User shall conduct the necessary housekeeping of his/her email at regular interval.
- Users should promptly report all suspected security vulnerabilities or problems that they notice with the email system to the designated ICT Team and or ISO.
- GOR has the authority to intercept or disclose or assist in intercepting or disclosing email communications.
- Users will not use any email account other than the one provided by GOR for transacting official information.
- Confidential information will be secured before sending through e-mail by way of compression, password protection or other advanced cryptographic means.
- Language used should be consistent with other forms of business communications
- GOR employees should treat electronic-mail messages with sensitive or confidential information as 'Confidential' and take due care as per the' information handling guidelines'.
- Users shall avoid opening mail from unknown users/sources and also avoid opening suspicious attachments or clicking on suspicious links.
- GOR shall restrict attachments size on the company mail system. Outgoing mail sizes are restricted to less than 5 MB.
- GOR reserves the right to monitor email messages and may intercept or disclose or assist in intercepting or disclosing Email communications to ensure that email usage is as per this policy.
- Users shall avoid sending or forwarding unsolicited email messages; "chain letters", "Jocks", "junk mail", etc.… from other internal users and external networks or other advertising material to individuals who did not specifically request such material (email spam).
- Users shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Users shall avoid unauthorized use, or forging, of email header information.

Staff should not:

- Use E-mail to manage staff where face-to-face discussion is more appropriate;
- Create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- Print out messages you receive unless you need a hard copy;
- Send large file attachments to E-mails to many addressees;
- Send an E-mail that the person who receives it may think is a waste of resources;
- Use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

4.21 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.

4.22 Internet Usage

- Users shall not use or access the internet for non-business purposes and restrict personal use to minimum limited to educational, knowledge and news sites. Users should strictly avoid visiting non-business, offensive and unethical sites which violate security policies.
- Users should not use Internet facilities to:
  - Download or distribute malicious software or tools or to deliberately propagate any virus
  - Violate any copyright or license agreement by downloading or distributing protected material
  - Upload files, software or data belonging to GOR to any Internet site without authorization of the owner of the file/ software/ data
  - Share any confidential or sensitive information of GOR with any Internet site unless authorized by Superior / Management
  - Users shall not post any GOR proprietary information or Internet share drives/Briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited and any violation will be subject to disciplinary process that includes legal consequences.
  - Post remarks that are offensive/aggressive/Insulting, obscene or not in line with GOR's policy on the subject.
  - Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the organization
  - In case such misuse of the Internet access is detected, Authorized personnel shall terminate the user Internet access and take other disciplinary action.
  - Users should ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.
  - Users shall be aware that their information systems(computer, internet, email, messenger, FAX and telephone conversations),its usage and information exchanged are not private and the Institution reserves the right to monitor and audit these on ongoing basis and during or after any security incident.
- Users must be aware that GOR accepts no liability for their exposure to offensive material that they may access via the Internet.
- Users should ensure that security is enabled on the Internet browser as per guidelines given below-
  - Configure browser not to remember web application passwords.
  - Set browser security setting to medium.

- Any bundled software that the user has obtained with mobile phones/ PDAs etc, should be explicitly approved by reporting head and ISO.
- GOR reserves the right to monitor and review Internet usage of users to ensure compliance to this policy. Any such monitoring will be authorized by ISMF and or ISO

5. Responsibility

The Group Director, Information and Communication Technology has responsibility for the implementation of this policy. ICT Management of MINEDUC are responsible for the maintenance and updating thereof, and must ensure adherence to this policy. All users of the MINEDUC ICT Systems are required to comply with this policy

6. Non-Compliance

MINEDUC reserves the right to audit compliance with this policy from time to time. Employees or contractors who breach the provisions of this policy will be disciplined in accordance with the disciplinary codes and procedures of MINEDUC. Any employees becoming aware of any breach of this policy should promptly and confidentially advise the persons to whom they report, to the managers of human resources, security or internal audit. MINEDUC reserves the right to suspend or permanently remove a user's access to some or all of the electronic communication facilities.

7. Glossary

Balanced Scorecard	A model of business performance management that balances measures of financial performance, internal operations, innovation and learning, and customer satisfaction
CobiT	Control Objectives for information and related Technology
Disaster recovery	The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure
Encryption	Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Encryption prevents any non-authorized party from reading or changing data.
Enterprise Architecture	A set of technical guidelines and standards to guide the enterprise in satisfying business needs. It comprises preferred technologies and vendors; templates, tools, methods and standards.

8. Authorisation, Approval, Review and Amendment Sheet

8.1 Approval and Amendments Sheet

This policy is approved by: Management of the Ministry of Education

This policy has been circulated to all department heads (Director Generals) and staff.

8.2 Review

In order to ensure that MINEDUC ICT assets are adequately protected and that this policy remains relevant, a review of this policy will occur in the first quarter of every year.

8.3 Records of Amendments

Version no.	Description of Amendment	Date