INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGERI

Accredited by Ministerial Order N° 005/2010/Mineduc of 16 June 2010

Scientia et Lux

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY-FINAL

February 2025

B.P. 155
Ruhengeri
Rwanda

T : +250 788 90 30 3
: +250 788 90 30 3
E : info@ines.ac.r
W : www.ines.ac.rw

INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGERI
B.P. 155, Ruhengeri | Rwanda
T: +250 788 90 30 30 | +250 788 90 30 32 | W: www.ines.ac.rw | E: info@ines.ac.rw

Table of Contents

1. Introduction

1.1. Preamble

The purpose of this Policy is to describe and document the ICT policies and procedures that will support INES-Ruhengeri goals and objectives within all the teaching, learning, research and administrative units. This geared towards increasing effectiveness and efficiency in all University functions. As such, the development of these policies took into consideration alignment to other existing University functional policies as well as globally recognized ICT practices. The Universitywill accordingly ensure the university-wide dissemination of this Policy to user group categories. The Policies will be reviewed periodically to ensure they remain relevant and aligned to thegoals of the University.

The adoption and utilization of Information and Communications Technology (ICT) within INES-Ruhengeri is aligned to the University Strategic Plan. The implementation of ICT requires an overall guiding framework to ensure that it's well-managed, complies with legal and regulatory requirements, creates value, and supports the realization of the University's objectives based on globally accepted best practice, guidelines and principles. In line with the above, the INES-Ruhengeri ICT Policy provides a structure for all the relevant ICT policies to support the achievement of the ICT Vision. Broadly, the policies here within spell out best practice, define roles and responsibilities of all user groups as well as provide guidance in the delivery, implementation and usage of ICT. Lastly, I wish to acknowledge the efforts of the Directorate for ICT Support in the coordination of the development of the ICT policy. We all have an obligation to the University to comply withthis Policy.

1.2. Statement of purpose

This policy seeks to guide developers and users of information and ICT resources on appropriate standards to be adopted at the INES-Ruhengeri. Its objectives include to:

- Provide guidance in developing a pervasive, reliable and secure *communications infrastructure* conforming to recognized international standards supporting all services in line with the priorities of the Institution;
- Provide a framework for development and management of ICT *network services* that shall ensure the availability, enhanced performance, security, and reduce the cost of running the ICT infrastructure;

- Establish information and implement *security* requirements across the INES-Ruhengeri's ICT infrastructure;
- Provide a framework, including guidelines, principles and procedures for the development and implementation of *Software Information System* projects in the INES-Ruhengeri;
- Guide the handling of *organizational information* within the ICT and the INES-Ruhengeri as a whole by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establish prudent practices on *Internet* and the INES- Ruhengeri *Intranet* use;
- Uphold the integrity and image of the INES-Ruhengeri through defined standards and guidelines for ensuring that the content of the Institution's *websites* is accurate, consistent and up-to-date;
- Serve as the direction pointer for the ICT's mandate in *supporting users*, empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches;
- To guide the process of enhancing user utilization of ICT resources through *training*;
- outline the rules and guidelines that ensure users' PCs and other *hardware* are in serviceable order, specifying best practices and approaches for preventing failure;
- Inform Departments carrying out projects financed in whole or in part by the INES-Ruhengeri, of the arrangements to be made in *procuring* the goods and services for the projects.

1.3. Scope of the INES-Ruhengeri ICT Policy

This policy applies to any person accessing, developing, implementing and, or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the Institution. The addresses include all Institution staff and students; any other organizations accessing services over INES-Ruhengeri ICT resources; persons contracted to develop, repair or maintain INES-Ruhengeri's ICT resources; and suppliersof outsourced ICT services. Adherence to this policy applies to all these and other relevant parties.

2. Network Development and Management Policy

2.1 Introduction to network policy

(a)The information and communications infrastructure at the INES-Ruhengeri has evolved

into a large, complex network over which the education, research and business ofthe INES-Ruhengeri is conducted. It is envisaged that the network will integrate voice, data and video, to form a unified information technology resource for the INES-Ruhengeri community. Such a network shall demand adherence to a centralized, coordinated strategy for planning, implementation, operation and support.

(b) The INES-Ruhengeri network functions shall be broken down into the following areas:

- Institution ICT Infrastructure Development
- INES-Ruhengeri backbone
- Campus Local Area Networks (LANs)
- Private networks
- Access to ICT facilities
- Connection to and usage of ICT facilities
- New or changed use of ICT equipment
- Monitoring of network performance.

2.2 Objectives of network policy

(a) The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy for the management of ICT infrastructure for theInstitution.

(b) This policy defines the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the Institution's ICT networks to ensure that, these networks are sufficiently adequate, reliable and resilient to support continuous high levels of activity.

2.3 Scope of network policy

This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of the Institution. These include all INES-Ruhengeri staff and students; any other organization accessing services over INES-Ruhengeri ICT networks; persons contracted to repair or maintain the INES-Ruhengeri's ICT networks; and suppliers of network services.

2.4 General network policy

2.4.1 The Network

The INES-Ruhengeri has developed and supported an INES-Ruhengeri-Local ICT network as a basic infrastructure service for the facilitation of sharing electronic information and resources by all members of the INES-Ruhengeri. This includes all staff and studentsof the INES-Ruhengeri, and other persons engaged in legitimate INES-Ruhengeri functions as may be determined from time to time.

2.4.2 Universal availability

(a) The INES-Ruhengeri network is designed and implemented in such a way as to serve those located at the INES-Ruhengeri campus.

(b) The ultimate goal is that every room in the INES-Ruhengeri in which research, teaching or support activities take place should be connected. And every member of the INES-Ruhengeri should have capability to access the INES-Ruhengeri ICT infrastructure.

(c) The INES-Ruhengeri network will form part of the general fabric or infrastructure of the INES-Ruhengeri.

(d) There will be one coherent network supporting access to all general information services provided to the Institution members. There may be separate private networks where they are warranted.

2.4.3 Reliability

(a) High levels of availability, reliability and maintenance will be major objectives in theconstruction and operation of the INES-Ruhengeri ICT network.

(b) The design and construction of the INES-Ruhengeri network will take into account emerging technologies and standards wherever possible.

2.5 INES-Ruhengeri ICT Infrastructure Development

2.5.1 Development plan

The INES-Ruhengeri ICT directorate will prepare a rolling five (5) year network development plan, advising on appropriate developments aimed at ensuring the adequacy of the INES-Ruhengeri's ICT infrastructure in future. This plan will take account of the INES-RUHENGERI's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

2.5.2 Implementation of new developments

(a) Prior to installation of the -live‖ situation, major network developments shall be -soak- tested‖ in off-line simulation.

(b) For up to two months after the live installation of the new development, the network provision that it is to be replaced shall, wherever possible, remain in place as a -fall- back‖ in the event of any subsequent failure of the new development when it is subject to actual user demand.

2.5.3 INES-Ruhengeri ICT network provision in new and refurbished buildings

(a) Network provision for new and refurbished buildings shall be made in accordance with the specification published from time-to-time by the INES-Ruhengeri ICT Department.

(b) All new buildings to be erected in the INES-Ruhengeri shall incorporate an appropriate structured data wiring system to allow connection to the INES-Ruhengerinetwork.

2.6 INES-Ruhengeri Backbone

2.6.1 Definition

The INES-Ruhengeri network will consist of several parts: "Backbone" systems, a collection of inter-building connections.

The INES-Ruhengeri Network Backbone will comprise an inter-building cabling system, together withone or more "Gateway" interfaces at each building or in the path to each building which will connect the Backbone to the network within each building.

2.6.2 Structure of INES-Ruhengeri backbone

(a) The INES-Ruhengeri Network Backbone shall connect, singly or severally, to buildings, not toindividual Departments or units.

(b) The planning, installation, maintenance and support of the INES-Ruhengeri Network Backboneshall be under the control of the ICT Department.

(c) Connection to the INES-Ruhengeri Network Backbone shall be approved by the Director ICTDepartment.

(d) The ICT Department shall adhere to and maintain copies of all relevant networking standards, and keep abreast of national and international developments in these standards.

(e) The INES-Ruhengeri Network Backbone at any particular point of time will be

aimed atfacilitating the traffic flow between connected buildings or networks.

2.7 Private networks

2.7.1 Definition

Departments or units may install, at their own expense, networks independent of the INES-Ruhengeri Network Backbone. Provided that the installation shall not interfere with the INES-Ruhengeri network. And provided the installation shall adhere to the INES-Ruhengeri policies and standards for installing and implementing such networks.

2.7.2 Structure of private networks

(a) Private Departmental networks may extend between buildings.

(b) The ICT Department may provide links for these networks but any extra expense incurredabove the INES-Ruhengeri Network Backbone requirements shall be charged to the Department.

(c) The ICT Department shall provide Campus Gateways for private Departmental networks where the private network caters for all the building occupants.

2.8 Access to ICT facilities

2.8.1 Communications rooms, cabinets and ICT network equipment

(a) All communications rooms and cabinets shall be locked at all times.

(b) Entry to communications rooms and cabinets, and interference with ICT networkequipment is strictly prohibited.

(c) Other than in an emergency, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICT Department. Any necessary access must have prior written consent of the Director of ICT Department

2.8.2 Access in an emergency

(a) In the event of a fire or other emergency, security staff and/or staff of the Estates Department and/or the emergency services may enter these areas, without permission, todeal with the incident.

(b) Where ICT network equipment is housed in accommodation used for another purpose, the arrangements for access by another user of that accommodation shall require the prior written consent of the Director of ICT Department. This consent shall

specifically exclude access by the other user to any communications cabinets or ICT network equipment located in the shared accommodation.

2.8.3 Contractors

(a) Contractors providing ICT network services must obtain the prior approval of the Director of ICT Department and shall obtain the appropriate authorization and the necessary Contractors' badge in compliance with procedures and regulations of the INES-Ruhengeri Security System.

(b) Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by appropriate INES-Ruhengeri ICT personnel.

2.8.4 Installation of cabling

All installations and changes of electrical power cabling in facilities housing ICT equipment shall be approved and managed by the Maintenance Department in consultation with the Director ICT in writing.

2.8.5 Installation of equipment

The specification of any equipment to be installed in communications rooms and cabinets and the installation of such equipment, shall require the prior written consent of the Director of ICT Department.

2.8.6 Network equipment

(a) Only designated members of the staff of ICT Department are authorized to install and maintain active network equipment including hubs, switches and routers connected to the INES-Ruhengeri's ICT networks.

(b) Where the Director of the ICT Department agrees that academic staff or the ICT Department's technical staff may install and maintain hubs and switches within local staff or student networks, such permission will in every case specifically exclude the point at which these hubs and switches connect to the INES-Ruhengeri's network infrastructure.

2.9 Connection to and Usage of ICT facilities

2.9.1 Connecting to the ICT network

(a) All connections to the INES-Ruhengeri's ICT networks must conform to the protocols defined by the ICT Department and with the requirements that apply to Internet Protocol (IP) addresses.

(b) Only designated members of staff of the ICT Department, or other staff authorized specifically by the Director of the ICT Department, may make initial connections of desktop services equipment to the ICT network.

(c) Computer workstations connected to the ICT network will not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the Director of the ICT Department has been obtained. Such consent will normally exclude all external access.

2.9.2 External access to servers on the backbone network

(a) External access means access by the external persons to the INES-Ruhengeri; access to the backbone network from external locations.

(b) Where specific external access is required to servers on the backbone network, the Director of the-ICT Department shall ensure that this access is strictly controlled and limited to specific external locations or persons.

(c) The Director ICT Department will monitor compliance with access arrangements as stipulated in this ICT Policy and the relevant ICT Security Policy on Server Security issued by the INES-Ruhengeri from time to time.

(d) Abuses of or failure to comply with these arrangements shall result in immediate restriction to or disconnection from the network.

2.9.3 Domain name services

All Domain Name Services (DNS) activities hosted within the INES-Ruhengeri shall be managed and monitored centrally, for the whole INES-Ruhengeri, by the ICT Department.

2.9.4 Electronic mail

Electronic mail or email shall be received and stored on central servers managed by the ICT Department f r o m where it can be accessed or downloaded by individual account holders.

2.9.5 Suspension and/or termination of access to ICT networks

(1) INES-Ruhengeri Employees

(a) A staff's access to the INES-Ruhengeri's ICT networks will be revoked automatically:
   i. at the end of his or her employment or research contract;
   ii. at the request of his or her Dean of Faculty/Head of Resource Centre/Head of Department or School or Head of Unit;
   iii. Where he or she has breached these regulations.

(b) The INES-Ruhengeri reserves the right to revoke staff's access to the INES-Ruhengeri's ICT networks where the user is suspended pursuant to a disciplinary investigation.

(c) The Administration Registrar will establish mechanisms whereby changes in employment status are communicated immediately to the Director of ICT Department so that these employees' computing and e-mail accounts can be suspended or deleted as appropriate.

Students leaving the INES-Ruhengeri

The Academic Registrar will notify the INES-Ruhengeri ICT directorate, by means of the regular student data transfer, of the names of students leaving the INES-Ruhengeri so that such students' computing, e-mail, printing and lending accounts can be deleted.

Procedures on Restriction of Use

(a) Appropriate procedures shall apply in restricting usage after a formal complaint has beenlodged or a breach of policy or rule has been reported or detected.

(b) Any breach of ICT policies shall be reported or communicated in writing to the Director,ICT.

(c) Upon receipt of any such complaint, the Director, ICT shall classify the complaint as -seriousǁ or -non-serious. ǁ A -non-seriousǁ complaint shall be defined as a breach of policy which does not subject the INES-Ruhengeri to a cost nor any risk.

(d) When a complaint is classified as -non-serious, ǁ the Director, ICT is authorized to impose any one of the following penalties:
   i. Suspension of the account for a minimum period of four weeks ii. Permanent disabling of the account

(e) When a complaint is classified as -serious,ǁ the Director, ICT shall refer the complaint to the ICT Committee for appropriate action. The possible penalties may be any one

ora combination of the following:

i. Notification of the suspension will be communicated to the relevant Dean and/or Head of Department or Section;
ii. Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Dean and/or Head of Department or Head of Section and a signed undertaking to abide by the Rules of Use shall be required before reinstatementof the account.
iii. Permanent disabling of the account shall be taken, where the severity of theoffence warrants such action.
iv. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the Director, ICT, which indicates that he or she was not involved in the transgression of the Rules of Use, or the Dean and/or the Head of Department or Head of Section requests the account be reinstated for courserelated work only (e.g. completion of an assignment). In this case the student or staff is required to sign an undertaking to abide by the Rules of use.
v. A system administrator within System admin (MIS User Support) can make a recommendation to disable an account to the Director, ICT. The director, ICT shall review the request and if there is considered to be, on the balance of probability, a transgression of the System Admin in ICT Rules of Use, the account shall be suspended.
vi. An account may also be suspended, if a request has been made to the Director, ICT from a systems administrator of another system, with a reasonable and acceptedcase for suspension.
vii. Users should note that suspension of access to ICT facilities also includes access tothe terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

Appeals

Students or staffs whose access has been suspended shall have the right to appeal in writing to the ICT Committee.

INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGERI * INES *

2.9.6 Internet Protocol (IP) addresses

(a) All equipment connected to the ICT networks shall be assigned unique IP addresses.

(b) The IP addresses assigned to equipment shall be recorded visibly on the casing of theequipment.

(c) The Communications and Networks Manager shall plan and allocate Blocks of IP addresses to different network segments and notify the relevant to ICT Director.

(d) The Communications and Networks Manager shall maintain a central record of IP addresses and may remove inactive IP addresses after six months.

2.9.7 Inventory control

As part of their audit responsibilities, Communications and Networks Manager shall be required to record in their local equipment inventory records the IP address assigned to each item of equipment for which they are responsible, together with the location of such equipment.

2.9.8 Connection of privately owned computers to the INES-Ruhengeri Network

Although members of staff and students may apply for an IP address, using the procedures in this Policy, to enable them to connect such computers or workstations to the INES-Ruhengeri network, permission shall be given only where the Communications and Networks Manager, ICT Department, is satisfied that the computer workstation meets the specification determined by the Director of ICT Department and that it poses no risk to the INES-Ruhengeri network.

2.9.9 Additional or changed equipment

(a) The Director ICT Department shall be advised in advance and at the earliest opportunity, of any plan to add items of desktop services equipment to or to replace or to relocate desktop equipment that are connected or that may require connection to the INES-Ruhengeri's ICT network.

(b) The Director ICT Department shall assess the likely impact on the INES-Ruhengeri's ICT networksof the proposed change. The Director ICT Department shall give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

2.9.10 External data communications

(a) All external data communications shall be channeled through the INES-Ruhengeri's

approved links.

(b) No external network connections shall be made without the prior written consent of the Director ICT Department.

(c) The installation and use of leased or private links on premises owned, managed or occupied by the INES-Ruhengeri shall require the prior written consent of the Estates Manager.

(d) The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the INES-Ruhengeri that are linked to the ICT network infrastructure, is prohibited, unless a proposal and justification for such connection has been authorized in writing by the Director, ICT.

2.9.11 Web cache provision

(a) The ICT Department shall be responsible for provision and management of INES-Ruhengeri's web cache facilities for incoming web traffic.

(b) All web access shall be set up to ensure use of the INES-Ruhengeri's web cache facility for incoming web traffic under the ICT Internet Usage Policy.

2.9.12 Web filtering

The Director ICT Department shall be responsible for the implementation of appropriate filtering facilities for web-based and non-web Internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value, where and when necessary in conformity with the ICT
Policy and relevant ICT Guidelines that promise efficient and high availability of Internet services to the majority of users.

2.10 New or changed use of ICT equipment

(a) The Director ICT directorate shall be advised in advance of any plan that involves a new use, a change of use or addition to the INES-Ruhengeri's ICT networks that might impact on the performance or security of the network.

(b) The Director ICT directorate shall assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the INES-Ruhengeri's ICT network. Such changes shall be effected after approval by the Director ICT Department.

2.11 Monitoring of network performance

The Network Manager, ICT directorate, shall monitor and document ICT network performance and usage and shall maintain regular monthly reports.

3. ICT Security and Internet Policy

3.1. Definitions of terms

(a) *Spam* - Unauthorized and/or unsolicited electronic mass mailings

(b) *Port scanning*- Attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.

(c) *Network sniffing* -Attaching a device or a program to a network to monitor and record data traveling between computers on the network.

(d) *Spoofing* -The deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.

(e) *Denial of service* -Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

(f) *Ping attack* - A form of a denial of service attack, where a system on a network gets-pinged, that is, receives an echo-request, by another system at a fast repeating rate thus tying up the computer so no one else can contact it.

3.2. Purpose

The purpose of this ICT Policy is to outline the acceptable use guidelines for ICT equipment and services at the INES-Ruhengeri. The intention of this policy to promote the INES-Ruhengeri's established culture of openness, trust and integrity. These are general guidelines on what can be done, and what should not be done, on the INES-Ruhengeri ICT Infrastructure in order to protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

3.3. Scope

This policy applies to permanent, temporary and casual staff, students, contractors, consultants, and other users of the INES-Ruhengeri ICT services, including all personnel affiliated with third parties. This Policy applies to all ICT equipment, software or other facilities that is owned or leased by the INES-Ruhengeri.

3.4. General use and ownership policy

3.4.1. Roles

(a) While the ICT Department is committed to the provision of a reasonable level of privacy, the ICT Department shall not guarantee confidentiality of personal information stored or transmitted on any network or device belonging to the INES-Ruhengeri. The data created and transmitted by users on the ICT systems shall always be treated as the property of the INES-Ruhengeri.

(b) The ICT Department shall protect the INES-Ruhengeri 's network and the mission-critical INES data and systems. The ICT Department shall not guarantee protection of personal data residing on INES-Ruhengeri ICT infrastructure.

(c) Users shall exercise good judgment regarding the reasonableness of personal use of ICT services. They shall be guided by ICT policies concerning personal use of ICT Internet, Intranet or Extranet systems. In the absence of or uncertainty in such policies or uncertainty, they shall consult the relevant ICT staff.

(d) For security and network maintenance purposes, authorized staff within the ICT Department shall monitor equipment, systems and network traffic at any time as provided for in the network and development policy.

(e) The ICT Department shall reserve the right to audit networks and systems on a periodic basis to ensure compliance with this ICT Policy.

3.4.2. Securing confidential and proprietary information

(a) INES-Ruhengeri data contained in ICT systems shall be classified as either confidential or non- confidential. Examples of confidential information include but are not limited to: payroll data, human resource data, and research data. Employees shall take all necessary steps to prevent unauthorized access to confidential information.

(b) Users shall keep passwords secure and shall not share accounts. Shared accounts are strongly discouraged. Authorized users are responsible for the security of their passwords and accounts. System level passwords shall be changed on a monthly basis; user level passwords shall be changed at least once every 3 months.

(c) All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host is unattended.

(d) Postings by users from the INES-Ruhengeri email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly the users and not necessarily those of the INES-Ruhengeri, unless posting is in the course and within the scope of official duties.

(e) All hosts connected to the INES-Ruhengeri Internet, intranet or extranet, whether owned by the useror the INES-Ruhengeri shall at all times be required to execute approved virus-scanning software with a current virus database.

(f) The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3.4.3. Unacceptable use

(a) Under no circumstances shall an employee, student, contractor or any staff be authorized to engage in any activity that is illegal under Rwandan or international law while utilizing the INES-Ruhengeri ICT resources.

(b) The following activities shall be prohibited. The list is by no means exhaustive, but is an attempt to provide a framework of activities that fall in the category of unacceptable use.

3.4.3.1. Unacceptable System and Network Activities

The following activities shall be strictly prohibited, with no exceptions:

(a) Violations of the rights of any person or company protected by Rwanda's copyright, trade mark, patent, or other intellectual property (IP) law and the INES-Ruhengeri's Intellectual Property Policy, other relevant policies, or the INES-Ruhengeri's code of conduct.

(b) Introduction of malicious programs into the network or server, for instance viruses, worms, Trojan horses or e-mail bombs.

(c) Sharing of the INES-Ruhengeri user accounts and passwords– users shall take full responsibilityfor any abuse of shared accounts

(d) Using the INES-Ruhengeri computing resources to actively engage in procuring or transmitting material that could amount to sexual harassment or constitute creation of a hostile work environment.

(e) Making fraudulent offers of products, items, or services originating from any the INES-Ruhengeri account.

(f) Causing a security breach or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which one is not an intended recipient or logging onto a server that one is not expressly authorized to access, unless this is within

(h) Super-user accounts such as —root‖ shall not be used when a non-privileged account can do.

(i) If a methodology for *secure channel connection* is available, that is technically feasible, privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPSec.

(j) Servers shall be physically located in an access-controlled environment.

(k) It shall be prohibited to operate servers from uncontrolled or easily accessible areas.

3.6.3. Monitoring

(a) All security-related events on critical or sensitive systems shall be logged and audit trails backed-up in all scheduled system backups.

(b) Security-related events shall be reported to the ICT information security officer, who shall review logs and report incidents to ICT management. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:

i. Port-scan attacks

ii. Evidence of unauthorized access to privileged accounts

iii. Anomalous occurrences that are not related to specific applications on the host.

3.7. Audit policy

For the purpose of performing an audit, any access needed shall be provided to members of the INES-Ruhengeri ICT audit team when requested. This access shall include:

(a) User level and/or system level access to any computing or communications device.

(b) Access to information (such as electronic or hardcopy) that may be produced, transmitted orstored on the INES-Ruhengeri ICT infrastructure.

(c) Access to work areas such as computer laboratories, offices, cubicles, or storage areas.

(d) Admission to interactively monitor and log traffic on the INES-Ruhengeri ICT networks.

3.8. Internal Computer Laboratory security policy

3.8.1. Ownership responsibilities

(a) All the INES-Ruhengeri units that own or operate computer laboratories shall appoint officers,designated as Computer Laboratory administrators, who shall take charge of their computer laboratories. A Computer Laboratory administrator shall be responsible for the day to day running of a Computer Laboratory, and shall be the point of contact (POC) for the ICT Department on all operational issues regarding the Laboratory. Heads of units

shall formally inform the ICT Department of the names and contacts of their computer Laboratory administrators.

(b) Computer Laboratory administrators shall be responsible for the security of their laboratories and their impact on the INES-Ruhengeri network, or any other network. They shall be responsible for overseeing adherence to this policy and associated processes.

(c) Computer Laboratory administrators shall be responsible for the Laboratory's compliance with all the INES-Ruhengeri ICT policies.

(d) Computer Laboratory administrators shall be responsible for controlling access to their computer laboratories; they shall ensure that only legitimate users can gain access to laboratory resources.

(e) The ICT Department reserves the right to interrupt laboratory connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk. For this purpose, Computer
Laboratory administrators shall be available round-the-clock for emergencies; otherwise actions shall be taken without their involvement.

(f) The ICT Department shall be furnished with records of all IP addresses and related configurations assigned to hosts in any computer laboratory. The Computer laboratory administrator or any other person shall, at no time, change these configurations without first notifying the ICT Department network management.

(g) Any INES-Ruhengeri unit that wishes to add an external connection to their Computer Laboratory whilst the laboratory is connected to the INES-Ruhengeri network shall provide a diagram and documentation of the proposed connection to the ICT Department with adequate justification. The ICT Department shall study such proposals for relevance, review it for any security concerns, and must approve before implementation is allowed to proceed.

(h) No computer laboratory shall replicate the core production services offered by the ICT Department. Production services shall be defined as all shared critical services running over the INES-Ruhengeri ICT infrastructure that generate revenue streams or provide customer capabilities. These services shall include, but shall not be limited to, World Wide Web (WWW) proxy services, E-mail services, Web hosting and FTP services. The ICT Department shall, alone, manage these services.

(i) The ICT Department shall address non-compliance waiver requests on a case- by-case basis and approve waivers if justified.

3.8.2. General configuration requirements

(a) All traffic between the production networks (networks connecting servers that run critical INES-Ruhengeri systems) and computer laboratories shall go through screening firewalls. Computer laboratory network devices (including wireless) shall not cross-connect a laboratory to a production network, circumventing screening firewalls.

(b) Computer laboratories shall be prohibited from engaging in port scanning, network auto-discovery, traffic spamming or flooding, and similar activities that may negatively impact on the overall health of the INES-Ruhengeri network and/or any other network. The general use and ownership policy shall apply.

(c) In computer laboratories where non- INES-Ruhengeri users are allowed access (such as computer training laboratories), direct connectivity to the INES production network from such laboratories shall be prohibited. In addition, no INES-Ruhengeri confidential information shall reside on any computing equipment located in such laboratories.

3.9. Anti-virus policy

(a) All Computers connected to the INES-Ruhengeri ICT network shall run the INES-Ruhengeri standard supported anti-virus software, and shall be configured to perform daily full-system and on-access scans.

(b) Anti-virus software and the virus pattern files shall be kept up-to-date always through scheduled daily automatic updates.

(c) Computer laboratory administrators and owners of computers, in consultation with the relevant ICT directorate personnel, shall be responsible for executing required procedures that ensure virus protection on their computers. Computers shall first be verified as virus-free before being allowed to connect to the INES-Ruhengeri network.

(d) Once discovered, any virus-infected computer shall be removed from the INES-Ruhengeri network until it is verified as virus-free.

(e) The following precautions shall be observed by all users to reduce virus problems. Users shall:

i. Never open any files or macros attached to emails from an unknown, suspicious or

untrustworthy source. All such emails shall be deleted immediately and emptied from trash folders

ii. Delete spam, chain, and other junk email without forwarding, in compliance with the general use and ownership policy.

iii. Never download files from unknown or suspicious sources.

iv. Avoid direct disk sharing with read/write access unless this is absolutely necessary.

v. Always scan removable media, including diskettes and memory sticks, from unknown sources for viruses before using.

vi. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

vii. In a computer where the anti-virus software is disabled, not run any applications that could transfer a virus such as email or file sharing. Such a computer shall be disconnected from the network.

viii. Periodically check for anti-virus updates and virus alerts because new viruses are discovered almost every day.

3.10. Physical Security policy

3.10.1. Required physical security

(a) *Security marking:* All INES-Ruhengeri computer hardware shall be prominently marked, either by branding or etching, with the name of the INES-Ruhengeri unit and name of office or computer laboratory where the equipment is normally located.

(b) *Locking of personal computer (PC) cases:* PCs fitted with locking cases shall be kept locked at all times.

(c) *Sitting of computers:* Wherever possible, computer equipment shall be kept at least 1.5 meters away from external windows in high-risk situations.

(d) *Opening windows:* All opening windows on external elevations in high-risk situations shall be fitted with permanent grills.

(e) *Blinds:* All external windows to rooms containing computer equipment at ground floor level or otherwise visible to the public shall be fitted with window blinds or obscure filming.

(f) *Door specification:* All doors giving access to the room or area with computer equipment both from within and outside the building, shall be, as a minimum, be fitted with supplementary metal grills.

(g) *Intruder alarm:* Rooms and buildings incorporating high-density computer equipment shall have intruder alarm detection equipment installed.

(h) *Location of intruder alarms:* Detection devices shall be located within the room or area and elsewhere in the premises to ensure that unauthorized access to the room orarea is not possible without detection. This shall include an assessment as to whether access is possible via external elevations, doors, windows and roof.

(i) *Detection device test:* A walk test of movement detectors shall be undertaken on a regular basis in order to ensure that all PCs are located within the alarm-protected area. This is necessary due to the possible ongoing changes in the position of furniture, screens and partitions, which may seriously impede the field of cover provided by existing detection devices.

(j) *Alarm confirmation:* Visual or audio alarm confirmation shall be provided for all conventional detection within the premise.

3.10.2. Computer server rooms

(a) Computer servers shall be housed in a room built and secured for the purpose.

(b) The computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

(c) No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

(d) Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

(e) Power feeds to the servers shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

(f) Where possible generator power shall be provided to the computer suite to help protect the computer systems in the case of a mains power failure.

(g) Access to the computer server rooms shall be restricted the authorized INES-Ruhengeri staff only.

(h) All non-ICT Department staff working within the computer server room shall be supervised at all times and the ICT management shall be notified of their presence and provided with

details of all work to be carried out, at least 24 hours in advance of its commencement.

3.10.3. Access control

(a) The system Administrator in charge of a particular system shall be the only authorized person to assign system, network or server passwords for relevant access to the system.

(b) The system administrator shall be responsible for maintaining the integrity of the system and data, and for determining end-user access rights.

(c) All supervisor passwords of vital network equipment and of those critical ICT directorate servers shall be recorded in confidence with the Director of ICT directorate, and the record safely stored under lock and key for emergencies.

(d) System audit facilities shall be enabled on all systems to record all log-in attempts andfailures, and to track changes made to systems.

3.10.4. Physical LAN/WAN security

(a) Switches

i. LAN and WAN equipment such as switches, hubs, routers, and firewall shall be kept in secured rooms. In addition, the equipment shall be stored in lockable air-conditioned communication cabinets.

ii. All communication cabinets shall be kept locked at all times and access restricted to relevant ICT staff only.

iii. Whenever legitimate access to communication cabinets is necessary, it shall be done with physical supervision of the responsible ICT personnel.

(b) Workstations

i. Users shall log out of their workstations when they leave their workstation for any length of time. ii. All unused workstations shall be switched off outside working hours.

(c) Wiring

i. All internal or external network wiring shall be fully documented. ii. All unused network points shall be de-activated when not in use.

iii. All network cables shall be periodically scanned and readings recorded for futurereference.

iv. Users shall not place or store any item on top of network cabling.

v. Where ducting is involved, fumigation and inspection shall be carried out regularly to curb damage to the cables by rodents.

vi. Redundant cabling schemes shall be used where possible.

(d) Monitoring Software

i. The use of monitoring tools, such as network analyzers or similar software shall be restricted to ICT Department staff who are responsible for network management and security only. Network monitoring tools shall be securely locked up when not in use.

(e) Servers

i. All servers shall be kept securely under lock and key.

ii. Library server and other servers of INES-Ruhengeri are maintained by ICT Directorate

iii. Access to the system console and server disk or tape drives of the production servers shall be restricted to authorized ICT directorate staff only.

(f) Electrical security

i. All servers and workstations shall be fitted with UPS to condition power supply.

ii. All switches, routers, firewalls and critical network equipment shall be fitted with UPS.

iii. Critical servers shall be configured to implement orderly shutdown in the event of atotal power failure.

iv. All UPS equipment shall be tested periodically.

(g) Inventory management

i. ICT directorate shall keep a full inventory of all computer equipment andsoftware in use throughout the INES-Ruhengeri.

3.11. Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and changes to hardware and software configurations.

3.12. Systems Backup Policy

3.12.1. Responsibility

All ICT directorate sections that operate key INES-Ruhengeri systems shall formulate and implement systematic schedules for performing regular backups on the systems in their custody.

The following cadre of staff shall carry full responsibility with regard to data backup implementation: The system administrators, application managers, INES-Ruhengeri archivist, MIS project leaders and database administrators. The responsible staff shall arrange to perform backups as scheduled at all times.

The ICT Security Officer shall be the principal back-up custodian. Back-ups of critical systems shall be documented with the ICT security office and handed over for safekeeping.

All responsible shall take necessary measures to ensure integrity, confidentiality and reliability of the back-ups.

3.12.2. Backup window

Backups for online systems shall be carefully scheduled so as to diminish any perceived degradation on system performance. Hence, back-up windows shall be scheduled at specific times of the day where the most minimal interruption on system services is likely. As a rule of thumb, all major backups shall be scheduled to run at night or during weekends, times when demand for system services is expected to be generally low.

3.12.3. Back-up inventory file

The ICT Department shall maintain a back-up inventory file, which shall document all backups carried out on critical INES-Ruhengeri systems. This shall provide mechanisms for quick monitoring and tracking of implementation of scheduled back-ups.

All relevant backups, whether stored in removable back-up media and/or on fixed media (hard-disks), shall be recorded in a back-up inventory file. See documenting data back-ups below for details.

The *back-up inventory file* shall be kept in a safe storage area, under custody of the ICT Security Officer.

3.12.4. Documenting data back-ups

The following information shall to be documented for all generated data backups:

(a) Date and time the data backup was carried out (dd/mm/yyyy: hh:mm).
(b) The name of the system or short description of the nature of the data
(c) Extent and type of data backup (files/directories, incremental/full).
(d) Backup hardware and software used (computer name, operating system (OS), version number).

(e) Sequence number if any (where multiple removable backup media are used).

(f) Physical location of the server and the logical path on file-system to the back-up area,when fixed media (hard-disks) are used.

(g) Data restoration procedures. This may be a separate booklet or set of guidelines

The above information shall be filed in the back-up inventory file. Removable media, inaddition, must carry proper labels documenting items (a) to (e).

3.12.5. Verification

There shall be a regular audit of all backup media. It is recommended that this exercise be carried out at least once every three months. A complete set of back-up media shall be restored, on a temporary location, and then inspected for accurate data reconstruction.

A report on the outcome of the audit shall be generated and recorded in the back-up inventory file.

3.12.6. Storage

(a) Removable backup media shall be stored in a locked fireproof safe within an access-controlled room.

(b) A complete copy of the current removable backup set shall be moved to secure offsite storage once every month.

3.12.7. Data restoration procedures

All step-by-step procedures needed in order to achieve complete data reconstruction and resumption of system operations from backups shall be documented. A hard copy of this document shall be filed in the back-up inventory file.

3.12.8. Back-up retention period and media rotation schedule

The retention period for back-up media shall be set in such a manner as to minimizethe risk of catastrophic loss of data at reasonable media cost.

The following guide, commonly known as the Grandfather-Father-Son (GFS) method, shall be adopted:

(a) Daily backups, known as the Son, shall be carried out on all, or selected days of the week;

(b) The last full daily backup in a week, known as the Father, shall be the weekly backup;

(c) Daily backups age only for the length of the week, hence the media shall be reused inthe coming week;

(d) The weekly backups shall be retained for a month and shall be reused during thenext month;

(e) The last full backup of the month is known as the monthly backup, or the Grandfather;

(f) The Grandfather backups become the oldest, and shall be retained for a year before themedia can be reused.

Back-up media must first be tested to guarantee their integrity before re-use. Media re-use must always begin with the oldest set.

3.12.9. Data Archiving

(a) ICT Department is obliged to maintain archives of data of critical INES-Ruhengeri systems fora time frame that is beyond the normal backup retention period, in case of future need to refer to the data by the INES-Ruhengeri or authorized Government agencies.

(b) For this purpose, in addition to normal backups, responsible staff shall arrange for a special backup scheduled at close of each financial year for all sensitive data on respective systems. Tapes used for this purpose shall be clearly documented and safely retained, with no intention of re-use, in a long-term storage facility.

3.12.10. Back-up media

(a) The following back-up media are recommended.

i. *Fixed computer hard drives*. These can be located over the network on a separate computer or, most preferably, on equipment using specialized storage technology such as Direct Attached Storage (DAS), Network Attached Storage (NAS) and Storage Area Networks (SANs). Use of these media is recommended where fast, very frequent and high capacity backups are required.

ii. *Compact Disc s (CDs), CDRW (Read/Write CD), Digital Video Discs (DVDs)* or a *ZIP drives*. Are recommended removable media for medium capacity backups or archives.

iii. *Tape cartridges (4mm tape, 8mm tape)*. Recommended removable media for use where high capacity backups and archives are required.

(b) For storage or transfer of small backups, *flash memory sticks* are recommended. *Floppy disks* are discouraged. Floppies have too low capacity and often develop errors over time, sometimes rendering backup data unrecoverable.

(c) Where backups are made on fixed media, redundant copies of the backup file shall be periodically made on removable media such as 4mm tapes, DVDs, or Read/Write CDs and stored at off-site storage area.

3.12.11. Back-up plans

Back-up plans, with the schedule of the general regular backup pattern for the key INES systems, shall be documented. The ICT security officer shall prepare this plan in conjunction with the persons responsible for back-ups. The ratified plan shall be authorized by the Director ICT and filed in the *back-up inventory file*. Persons responsible for back-ups shall carryout all back-ups as scheduled on the back-up plan, but may also stipulate additional event-dependent intervals where necessary.

3.13. Internet Usage Policy

(a) All software used to access the Internet shall be part of the INES-Ruhengeri standard softwaresuite or approved under the ISO standard.

(b) All users shall ensure that Internet access software shall incorporate the latest security updates provided by the vendors.

(c) All files downloaded from the Internet shall be scanned for viruses using the INES-Ruhengeri's corporate anti-virus software suite with the latest virus detection updates.

(d) All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.

(e) Accessed Internet sites shall comply with the INES-Ruhengeri General Use and Ownership Policy.

(f) Internet access traffic through the INES-Ruhengeri ICT infrastructure shall be subject to logging and review. (g) The INES-Ruhengeri Internet access infrastructure shall not be used for personal solicitations, or personal commercial ventures.

(h) All sensitive INES-Ruhengeri materials transmitted over the Internet shall be encrypted.

(i) Official electronic files shall be subject to the same rules regarding the retention of records that apply to other documents and information or records shall be retained in accordance with INES-Ruhengeri records retention schedules.

INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGERI * INES *

4. User Support Policy

4.1. Definition of terms

(a) *ICT project*: Any ICT work or undertaking that happens only once, and has a clear beginning and end, and is intended to create or deploy a unique ICT technology, product, knowledge or service.]

(b) *Basic Operation Unit (BOU) Laboratory*: 3 or more computers used by academic, non-teaching staff, or students for general use, research, in a classroom setting, or as a component of a class and operated by an autonomous Department, school, faculty, institute, Centre or other unit of the INES-Ruhengeri.

(c) *Hardware*: All INES-Ruhengeri-owned computer and peripheral equipment (such as printers, scanners, CD-ROMS (Read only memory compact discs), network cards and multimedia equipment). Excluded from such equipment would be equipment that is already under an existing service contract, warranty, nonstandard ICT equipment for which only advisory information shall be provided.

(d) *Tools and equipment*: The stock of shared tools maintained both centrally at ICT and within individual campuses for use by the support personnel.

(e) *ICT user support services*: ICT services directed at ICT users to enable users to effectively exploit ICT technologies, products and services available at the INES-Ruhengeri. These shall mean all activities, carried out by the support personnel involving setup, creation, procurement and acquisition, installation and deployment, repair and training on ICT technologies, and products and services, with the aim of assisting users to maximize expected utility and benefit

(f) *Support coverage*: Support Site and deployment of support personnel in accordance with the assessed support load per site.

(g) *Hardware support*: Attending to problems associated with hardware categories as listedunder the support policy.

(h) *Software support*: Attending to problems associated with software categories as listed under the support policy.

(i) *MIS support*: support for corporate systems used by the INES-Ruhengeri.

4.2. Introduction

The ICT Department acquires, develops and produces a variety of ICT technologies, products

and services in response to the academic business and related requirements of the INES-Ruhengeri. Upon production, these require are distributed (or made available) to users. Thereafter, continuous and carefully tailored support is necessary in order for the users to fully exploit them. A policy guideline is necessary for this support.

4.3. Policy objective

(a) A guideline for the ICT User Support Service for enabling *bona fide* INES-Ruhengeri ICTusers to productively exploit provided INES-Ruhengeri ICT resources.

(b) Specific Services include: General User Support Service; PC and User Peripheral Service; Hardware Maintenance Service; Network Support Service; ICT Staff Professional Training Service; ICT User Training Service; Operationalization of ICT Projects.

4.4. Scope

This guideline shall steer the activities of producers and consumers of ICT technologies, products and services across the INES-Ruhengeri.

4.5. Policy Statements

4.5.1. INES-Ruhengeri ICT projects and services

The Director, ICT shall ensure that ICT Support services to assist INES-Ruhengeri ICT Users with technical and logistical support in the implementation (or roll-out) and operationalization of ICT Technologies, Projects, Products; and Services.

4.5.2. Advocacy

The ICT Centre through User Support services shall provide users with consultancy services on any ICT matter; it shall provide technical representation in all ICT related meetings and committees; it shall communicate relevant User Support information to users, and provide them with liaison interface (or escalation point) to the greater ICT Department.

4.5.3. Support Coverage

(a) Support sites shall be designated by campus and to some extent by function. These shall be as detailed in the schedule of support coverage in the standards document.

(b) The ICT Support function shall provide qualified support personnel at each INES-Ruhengeri campus. ICT Support personnel shall be deployed in accordance with the

assessed support load per support site (or campus). The load shall be proportional to the extent to which ICTs are in use, determined mainly by the expansion of the INES-Ruhengeri network and number of users there off.

4.5.4. Procurement Support

The ICT User Support function shall assist users in deriving the technical requirements and specifications of all ICT acquisitions and purchases. Other acquisitions and purchases must meet the minimum specifications as outlined in the ICT procurement policy for all hardware, software, services and consumables in order to guarantee support by ICT under the categories outlined above. The ICT User Support function shall verify all ICT acquisitions and purchases.

4.5.5. Infrastructure support

The ICT User Support function shall assist users in carrying out surveys, design, requirements, specifications, and preparation equipments, material acquisition and supervision of implementation of all ICT infrastructures at the INES-Ruhengeri.

4.5.6. Hardware Support

(a) The User shall be responsible for daily care and basic routine maintenance of ICT hardware under their care. ***(Refer to ICT Maintenance Equipment Policy)***

(b) On a second level, the ICT Support Function shall support the hardware categories that are commonly required by users in their offices, computer rooms, laboratories and lecture theatres to perform their job responsibilities. These shall include servers, desktop computers, laptop computers, printers, scanners, digital cameras, liquid crystal display (LCD) projectors, *PDAs* (palm or pocket PC), UPSes, network access hardware, among others.

4.5.7. Software and MIS Support

(a) ICT Support shall support software categories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture theatres to perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement and ICT MIS development policies for software and MIS in order to guarantee support by ICT ***(Refer to Software Development, Support and Use Policy)***. The supported categories shall include PC Operating Systems, PC Applications and Client Software,

Security and Antivirus, PC backup support, among others.

4.5.8. ICT services support

(a) The ICT Department shall support ICT services that are commonly required by users in their offices, computer rooms, laboratories and lecture theatres to adequately perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement policy for software in order to guarantee support by ICT.

4.5.9. Departmental Support

(a) The ICT Department shall act as the second level support to the existing Computer Laboratory Attendant or Administrator for INES Basic Operation Units (BOU) with ICT personnel. The ICT Department shall be available to consult or to help with significant problems.

(b) The ICT Centre shall not be available to provide basic and routine cleaningand simple troubleshooting for machines except where such computer laboratories are directly owned by the ICT.

4.5.10. Network devices

The ICT Department shall own core network active devices such as switches, routers, bridges, gateways and related equipment including enclosures, and shall be responsible for the following:

(a) Creating and maintaining adequate operating environment (floor space, climate control, ventilation, backup power supply) for the equipment.

(b) Routine maintenance and upgrade of the equipment.

(c) Advising on all expenses incurred during repair, maintenance, and upgrade.

4.5.11. Printing facilities

A Basic Operation Unit in the INES-Ruhengeri shall implement a centralized printing facility at which most print jobs shall be processed. This shall be equipped with at least one print device of appropriate specification that shall be administered from a print server. The facility shall also be equipped with at least one photocopier.

4.6. Escalation of support requests

Where necessary the ICT Support Function shall escalate user support requests to appropriate

ICT Department sections and to other INES-Ruhengeri functional units.

4.7. Support resources

The Basic Operation Unit shall provide Office and workshop space, furniture, and basic office amenities.

4.7.1. Tools and equipments

INES-Ruhengeri shall have a stock of support tools consisting of items as listed on the schedule dedicated for the support work within. In addition, a stock of shared tools shall be maintained centrally at ICT.

4.7.2. Dress and gear

Support personnel shall be supplied with protective and safety clothing and gear suitable for the tasks involved in the support activities. These shall include items such as overalls, dustcoats, dust masks, safety gloves and the management of the ICT Department from time to time may determine other items.

4.7.3. Logistical Resources

(a) Towards realizing the set support standards such as turn-around time and low down time, ICT shall ensure availability of logistical resources for transport to ensure rapid movement between support sites, and, communications to ensure contact between support personnel.

(b) Transportation: There shall be sufficient transport services available for the support function.

(c) Communication: Support personnel shall be equipped with appropriate communication equipment to maintain effective contact with one another in the course of duty.

4.7.4. Enforcement

(a) The enforcement of this policy shall be the responsibility of the ICT Department.This shall be ensured through strict adherence to the ICT standards.

(b) Violations will be addressed by established INES-Ruhengeri and National Legal Mechanisms.

(c) Where required and applicable, an ICT Department Committee shall provide oversights, insights and guidance in case of any violation.

5. ICT Equipment Maintenance Policy

5.1. Definition of Terms

(a) *Hardware*: This shall mean all INES-Ruhengeri owned computer and peripheral equipment(such as printers, scanners, CD-ROMS, network cards and multimedia equipment). Excluded from such equipment shall be equipment that is already under an existing service contract, warranty, and non-standard ICT equipment and for which only advisory information shall be provided.

(b) *Tools and equipment*: The stock of shared tools maintained both centrally at ICT Department and within individual campuses for use by the support personnel.

(c) *Brand name system*: A brand name computer (both hardware and software) is based on a particular company's architecture aimed at providing a unique service to its customers.

(d) *Clone or semi brand system*: A clone is a computer system (both hardware and software) based on another company's system and designed to be compatible with it.

5.2. Introduction

The INES-Ruhengeri recognizes the important role of the Maintenance Section in providing qualityservices to its users, by ensuring that their equipment is well maintained and repaired ingood time. This policy will guide the maintenance personnel at the INES-Ruhengeri Central Facility as well as those at the various campuses.

5.3. Policy objective

This policy document outlines the rules and guidelines that ensure that users' PCs and related hardware are in serviceable order. It specifies best practices and approaches in ICT equipment maintenance.

5.4. Scope

(a) This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the INES-Ruhengeri, including all

INES-Ruhengeri staff and students; and any other organization accessing INES ICT services including persons contracted to repair or maintain the INES-Ruhengeri 's

ICT equipment and suppliers of such equipment.

(b) This policy specifies the general approach that the maintenance centre shall use in providing users with the facilities; services and skills to enable them to utilize the maintenance centres productively.

(c) It describes the steps that are to be followed by the maintenance personnel in the process of providing repair support.

5.5. Policies

5.5.1. Operational logistics

(a) Operationally, users shall resolve basic problems as the first level of maintenance and support.

(b) At the second level, the OIC in each campus shall offer support to the users on issues they cannot resolve.

(c) At the third level specialist Maintenance Engineers at the Central Facility shall handle issues escalated from various campuses.

(d) The fourth and final level should enable the Central Facility to work in liaison with vendors, suppliers and hardware manufacturers to repair and/or replace faulty equipment.

(e) The Central Facility shall be charged with the responsibility of enforcing any maintenance contracts, agreements and warranties.

5.5.2. Hardware Maintenance

The ICT Department shall maintain and support the supportable hardware[2]categories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture theatres to perform their daily responsibilities. Users shall follow the ICT procurement policy for hardware in order to guarantee support by ICT.

5.5.3. Privately owned computer equipment/peripherals

The ICT Department shall not take responsibility for the replacement, repair or upgrade of privately owned equipment/peripherals.

5.5.4. Computer Systems and Peripherals

In the case of computer systems, Departments that purchase the equipment shall be responsible for the following with the aid of ICT Centre:

(a) Adequate operating environment (floor space, climate control, ventilation, and backup power supply) for the system.
(b) Installation and administration of the system.
(c) Routine maintenance and upgrade of the system.
(d) All expenses incurred during repair, maintenance, and upgrade.
(e) Full compliance with the INES-Ruhengeri's Procurement and Disposal Policy/Act.
(f) Full compliance with the INES-Ruhengeri's security policy, including installation and regular updateof the anti-virus software.
(g) Supplies for spares to support such systems and peripherals shall be the responsibility of the Department.

5.5.5. Tools and equipment

Every campus shall have a stock of support tools that is continually being stocked. In addition, a stock of shared tools shall be maintained centrally at the ICT Department.

5.5.6. Campus workshops

Every campus shall have a designated repair facility. This facility shall take the form of a room reserved for the purpose of conducting all hardware repair and maintenance activities. The ICT Department personnel in the campus shall have custody of such facility.

5.5.7. Preventive maintenance

A schedule for maintenance shall be drawn, recognizing every piece of hardware. Preventive maintenance shall be carried out according to the recommendations of the manufacturer of the hardware, in terms of frequency and method of maintenance. However, where justified by the case, service shall be provided on the basis of request.

5.5.8. Outsourced Service Agreement for Critical Equipment

Equipment not supportable by ICT Department shall as far as possible be placed on maintenance contracts.

5.5.9. Obsolescence of hardware

ICT hardware shall be declared obsolete according to the recommendations of the manufacturer. The hardware maintenance team shall periodically conduct maintenance to identify, retire and replace the hardware categorized as at -end-of-life.

5.5.10. Warranty guidelines

Maintenance staff at the ICT directorate shall facilitate the repair and maintenance of equipment under warranty. They shall keep accurate records of the warranty of the individual items of equipment and use such information when needed to operationalize the warranty and/or guarantee for the equipment.

6. ICT Training Policy

5.1 Introduction

A variety of services are developed and produced by the ICT directorate in response to the business requirements of the INES-Ruhengeri. Upon production, these services are distributed (or made available) to users. Thereafter, continuous and carefully tailored training support is necessary in order for the users to fully exploit them. Policy guidelines shall be clarified for such training.

5.2 Objective

The objective of this policy is to outline the guidelines that serve as the guiding reference when planning for, organizing and conducting ICT training at the INES-Ruhengeri.

5.3 Scope

(a) This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the INES-Ruhengeri, including all INES-Ruhengeri staff and students; and any other organization accessing INES-Ruhengeri ICT services including persons contracted to repair or maintain the INES's ICT equipment and suppliers of such equipment.

(b) This policy specifies the general approach to the training of all INES-Ruhengeri staff and students; and any other organization accessing INES-Ruhengeri ICT services, as the primary users of ICT services.

(c) It addresses the training content and methodology for ICT users.

5.4 Policy Statements

5.4.1 ICT Literacy

It shall be mandatory for all INES-Ruhengeri staff to be literate users of ICT services, the level of literacy being in line with the demands of their job functions. Training shall therefore focuson building skills in users making them effective in exploiting provided ICT resources.

5.4.2 Mode of Training

(a) External ICT training shall be organized by the ICT directorate in response to need as may be assessed from time to time when training is not possible within the INES-Ruhengeri.

(b) Internal ICT user training targeting the INES-Ruhengeri community shall be scheduled on a continuous basis and shall be conducted both in the campuses and at the corporate training computer laboratory at the ICT directorate.

5.4.3 Trainees

(a) The ICT directorate shall jointly with user Departments nominate trainees for external ICT training when the need for such training arises.

(b) Every Officer in Charge of Campus (OIC) shall jointly with the user Departments intheir campus and in response to assessed needs nominate trainees early in every quarter and forward the list to the user support manager. The number of trainees shall be as targeted in the Strategic Plan for the campus or unit. The operating unit shall make the necessary arrangements to facilitate trainees drawn from such units.

5.4.4 Training Resources

The ICT directorate shall in liaison with either the Project Manager or the producer of the relevant services identify the appropriate trainers for the training. These shall be as demanded by the needs of the scheduled training.

The ICT Department jointly with the user Departments shall provide necessary resources to facilitate the training

5.4.5 Training needs and Curriculum Development

Officer in charge of Campus (OIC), Project Managers and service developers shall establish ICT training needs in liaison with user Departments and service consumers. In cases where the ICT Department is not well placed to train in a given area, the ICT directorate shall identify and recommend appropriate training and work out the cost for competent trainers.

(a) The ICT directorate shall develop curricula for all training including developmentof source material. To this end, the ICT directorate shall:

i. Recommend curriculum for all external training

ii. Where possible provide training materials on-line via the INES-Ruhengeri website.

iii. Where possible conduct on-line assessment tests and examinations.

(b) Where external training is sourced, the ICT directorate shall jointly with theexternal training agent, customize the content to meet the training needs of the users.

5.4.6 Acknowledgement of training

The ICT directorate shall issue certificates on successful completion of training andexamination.

7. Database administration policy

7.1. Terms and definitions

a) *Database* - software used for management of data objects.

b) database administrator (DBA)–The person in charge of administration and management of a database

c) *Production database* – database for applications that have gone through the system life cycle as defined in the Software Development Policy.

d) *Replication database* – database used for maintaining a complete copy of the productiondatabase.

e) *Development database* – database used for development of applications before deployment to the integration database.

f) *Integration database* – database used for testing and integrating applications before deployment into the production environment

g) *Education database* - database used for use by students and staff of the INES-Ruhengeri.

7.2. Introduction

Contemporary Information Systems (IS) rely on the use of emerging database technologies for storage and manipulation of data. Several challenges arise in the utilization of these database technologies, including:

(a) availability of the database service to the intended customers

(b) flexibility in terms of access through the use different interfaces

(c) administration and management of the same service

7.3. Objectives

These policies have been developed in order to achieve the following goals:

(a) Provide the best possible database service to the INES-Ruhengeri Management Information Systems application development and administration groups as well as the INES-Ruhengeri academic and student community in general.

(b) Allow the flexibility required to rapidly develop information and communication technology solutions unhindered, while at the same time providing access to expert consultation when desired.

(c) Ensure that the INES-Ruhengeri's data resources are firmly controlled based upon known requirements and that data changes can be audited.

(d) Enhance the efficiency with which database applications are developed, deployed and executed.

7.4. Scope

(a) This ICT Policy document shall be a point of reference between the Database Administrators (DBAs), on the one hand, and application developers, Project Leaders, database users and students, on the other hand, in usage, administration and management ofthe database service within the INES-Ruhengeri.

(b) The INES-Ruhengeri database services, maintenance of user accounts; backup, and recovery shall be carried out in accordance to the ICT security policy, while training will be in accordance with the User Support and Training policy.

(c) The MIS application process will be carried out in accordance with the MIS Software Development Policy.

7.5. Policy Statements

7.5.1. Services

An appropriate channel of communication that allows the DBA to receive and respond to requests for database services shall be available e.g. email and memo.

The DBA shall provide the following services:

a) Authorization and Access Control

(i) Authorization and data control: Access to the production (and replication) databases shall be restricted to production applications and through authorized reporting tools.

(ii) Authorization outside of these applications shall be approved by the client controlling the data and will be maintained and controlled by DBA.

(iii) Access to the development and integration, as well as education databases shall be given to developers, students or members of staff working on current UMIS (or otherwise) projects or for developing their database skills.

(iv) Developers shall have a special role for functional development and integration databases that they support.

b) Development Support

(i) DBA shall provide support to the development group.

(ii) Support activities shall include, but shall not be limited to the following areas: database design or re-design; application design; application (SQL) performance analysis; disk space analysis; data recovery analysis; and data and process modeling.

c) Operational Support

Operational support shall include: production application analysis; data monitoring and reorganization; recovery management; space management; performance monitoring; exception reporting; application system moves to production. These ongoing activities must occur in order for data and applications to quickly move through the Development Life Cycle process and perform efficiently in the production environment.

d) Monitoring and tuning

(a) Once the data and applications have been moved to production, the Database Administrator (DBA) shall utilize various tools to monitor their operation.

(b) The DBA shall make modifications to the data size allocations, reorganization frequency, and copy and frequency only liaison with the relevant Project Leader.

(c) The DBA shall bring application inefficiencies to the attention of the relevant Project Leader and make recommendations, if desired, on ways to tune them and make them more efficient.

7.5.2. Service Level Agreements (SLAs)

The DBA shall respond to service request in accordance to the ICT Department Service Charter

8. Procurement Policy

8.1. Definitions

(a) *Department*: The INES-Ruhengeri is made up of numerous units that have their own procurement needs. These units control their own resources and can therefore procure goods and services. These include Faculties, Academic Departments, Service Departments, Centres and administrative offices. In this policy, the term Department means the procuring entity within the INES-Ruhengeri.

(b) *ICT Goods and services*: The ICT goods and services to be provided by the selected Bidder under the Contract (such as the supply of any major hardware, software, or other components of the required Information Technologies specified, or the performance of any related Services, including software development, transportation, installation, customization, integration, commissioning, training, technical support, maintenance or repair).

(c) *Technical specifications*: A document intended primarily for use in procurement, which clearly and accurately describes the essential and technical requirements for items, materials, information systems or services, including the procedures by which it will be determined that the requirements have been met.

(d) *Emergency*: This is a sudden unforeseen crisis usually involving possible negative consequences, requiring immediate action, in this case undertaking a sudden procurement.

This will be done through obtaining quotations upon the approval by the Tender Board Committee.

(e) *Project*: This is the activity of establishing and assembling all the specifications and cost elements with a view to initiating an acquisition within an agreed scope.

(f) *Quotation*: This will mean a statement of the present going market price for goods or services including the accompanying terms as provided by the intending supplier.

8.2. Introduction

The rules and regulations governing procurement of goods and services for the Republic of Rwanda and which are applied by the INES-Ruhengeri shall form the basis of these policy statementson procurement of goods and services.

(a) The ICT Department shall assist the Departments with preparation of technical specifications for the purpose of procuring goods and services related to ICT whenever need arises.

(b) The ICT Department shall also assist the Procurement office in cases of emergencies to identify reputable companies or registered providers to reduce any delay in procurement.

(c) The rights and obligations of the Department and the suppliers of goods and services for the project are governed by the procurement regulations, the procurement policy, the bidding documents, and by the contracts signed by the INES-Ruhengeri with the suppliers of goods and services, and shall prevail in the event they are inconsistent with this policy.

8.3. Objectives

The objective of this policy is to inform and guide Departments procuring ICT related goodsand services at the INES-Ruhengeri.

8.4. Scope

(a) The responsibility for the implementation of the project, and therefore for the award and administration of contracts under the project, rests with the INES-Ruhengeri. The ICT Department, shall endeavor to ensure that various Departments have followed the correct procedure for procurement of ICT related goods and services.

(b) The ICT Department shall assist the Departments with preparation of technical specifications whenever need arises. The principles of economy and efficiency in the procurement of the goods and services involved shall guide the process. The

importance of transparency in the procurement process is essential.

(c) The procedures shall conform to the INES-Ruhengeri's rules, regulations and obligations and ensure that projects for various Departments are pursued diligently and efficiently. The procedures shall also ensure that the goods and services to be procured meet the following criteria:

i. Are of satisfactory quality and are compatible with the balance ofthe project;
ii. Will be delivered or completed in timely fashion; and,
iii. Are priced so as not to adversely affect the economic and financial viability of the project.

8.5. Policy Statements

It is important for various Departments to follow the procurement policy set by the INES-Ruhengeri for the Procurement of goods and services. The following policy statements shall govern the units or entities of the INES-Ruhengeri in the procurement of ICT goods and services:

(a) Identification of the needs and the justification for procurement of goods and services.
(b) Development of the technical specification with the help of the ICT Department and ensure the specification used by the user Department is up-to- date and uses state of art technology and not older than three months.
(c) Adhere to the procurement policy of the INES-Ruhengeri.
(d) Comply with the financial regulations of the INES-Ruhengeri.
(e) All ICT goods and services shall be delivered to the ICT Department located in INES-Ruhengeri Campus or wherever it may be headquartered from time to time.
(f) Inventory of all the ICT goods and services procured by the various Departments must be forwarded to the Director of the ICT Department for record keeping purposes.
(g) ICT Department shall:
    i. Check the delivery schedule.
    ii. Examine and test the compliance of the goods to technical specifications inaccordance with the contract awarded to the supplier.
    iii. Install necessary software and configure the PCs, printers and laptops and assign IP addresses for unique identification of delivered equipment.

8.6. Replacement of Goods and Services

The life cycle of the goods and services is dependent on the type of the goods and services procured by the INES-Ruhengeri. On average, hardware shall be replaced after every five years if funds are available. While for software the life cycle is dependent on the release of the new versions in accordance with the software maintenance agreement. The disposal of obsolete equipment shall be governed by the INES Procurement Policy.

9. CCTV Camera at INES-Ruhengeri

The use of CCTV cameras at INES-Ruhengeri serves multiple purposes, contributing to both the security and academic integrity of the institution. Strategically installed surveillance cameras enhance campus safety by monitoring: entrances, academic buildings, laboratories, and public spaces. This proactive approach helps deter unauthorized activities, ensuring a secure environment for students, staff, and visitors. The cameras also assist in incident investigation by providing valuable footage when necessary, promoting accountability across the campus.

9.1. Places where to install CCTV cameras

At INES-Ruhengeri, CCTV cameras should be installed in key areas to ensure campus safety and security. These include all main entrances and exits, administrative buildings, academic facilities such as classrooms, examination rooms and laboratories, library spaces, and parking and any other place with INES-Ruhengeri facilities. Cameras should also cover common areas like hallways, corridors, and outdoor spaces where large gatherings occur. Strategic placement in these locations helps monitor foot traffic, prevent unauthorized access, and deter criminal activity. Additionally, cameras may be placed in IT rooms, server areas, and other high-security zones to protect sensitive equipment and data. All cameras should be positioned to capture activity without infringing on individual privacy, ensuring a balance between security and privacy protection.

9.2. Place where CCTV cameras are restricted

At INES-Ruhengeri, the installation of cameras is restricted in areas where privacy is paramount. Cameras should not be installed in locations such as restrooms, changing rooms, residential dormitories, or any other spaces where individuals have a reasonable expectation of privacy. Additionally, cameras should not be placed in faculty or staff offices unless expressly approved for security purposes by the administration and with the consent of the occupants. These restrictions

ensure that while the campus remains secure, the privacy and dignity of students, staff, and visitors are fully respected in accordance with legal and ethical standards.

9.3. Access to camera footages

At INES-Ruhengeri, camera footage is important for ensuring campus security, safety, and academic integrity. Access to this footage is strictly regulated to protect the privacy and rights of individuals on campus. Only authorized personnel, such as security staff, campus administrators, and IT Department representatives, may access the footage. These individuals must have a legitimate reason, such as investigating a security incident, conducting a safety audit, or reviewing technical issues with the camera system. All access must be logged and monitored to ensure compliance with institutional policies and legal regulations.

Footage obtained from campus cameras will not be shown to the public unless required by law or in circumstances where the institute deems it necessary for transparency regarding serious security incidents. In such cases, the decision to release footage will be made by senior administration, in consultation with legal advisors, to ensure that the privacy of individuals is respected and that the footage is not misused. Public access to footage will only be granted when it serves a clear institutional purpose, such as addressing a public safety concern or responding to media inquiries in relation to a significant event on campus.

9.4. Circumstances where CCTV cameras will be consulted

CCTV cameras at INES-Ruhengeri may be consulted and shared with students under specific circumstances where there is a need to investigate theft or loss of valuable items. If items such as laptop cables, mobile phones, laptops, tablets, cameras, laboratory equipment books, or any other valuable personal belongings are reported stolen or missing, CCTV footage may be reviewed to identify suspicious activity and resolve the issue. In case thief is caught, security officer and dean of students will act according to what code of conduct says. Additionally, the cameras may be consulted in cases involving damage or theft of institutional property, including library materials, classroom technology, or office supplies. The review of such footage will be conducted with administrative approval to ensure transparency and fairness, and only relevant parties, such as the affected students and security personnel, will be consulted during the investigation process. This ensures that privacy is maintained while protecting the safety and property of the campus community.

9.5. CCTV Cameras footage backup and management

At INES-Ruhengeri, CCTV footage will be stored for a designated period to ensure the security and integrity of the campus, typically retained for a minimum of 30 days unless required for ongoing investigations. After this period, the footage will be automatically overwritten to optimize storage capacity. However, in the event of a reported security incident, specific footage may be archived for a longer duration until the issue is resolved. Regular backups of critical footage will be conducted to prevent data loss and ensure continuity, with backups stored securely and accessible only to authorized personnel. This policy ensures a balance between security needs and efficient data management, while complying with legal and privacy standards.

10. Use of Use of virtual meeting platforms at INES-Ruhengeri

The use of virtual meeting platforms at INES-Ruhengeri is integral to facilitating efficient communication and collaboration within the academic and administrative community. These platforms, such as Zoom, Microsoft Teams, and Google Meet, enable remote interactions, allowing students, faculty, and staff to participate in lectures, meetings, seminars, and other institutional activities, regardless of their location. The adoption of virtual meeting platforms ensures continuity in learning and operations, particularly in times when in-person meetings are not feasible. It also supports the institute's commitment to leveraging technology for enhanced accessibility, flexibility, and engagement in academic and non-academic endeavors. The policy governing the use of these platforms ensures that they are used responsibly, securely, and for purposes aligned with the institution's educational goals and operational needs.

10.1. Restrict of using free virtual meeting platforms

The use of free virtual meeting platforms, such as Zoom's free version or Google Meet's basic tier, is restricted during official meetings at INES-Ruhengeri due to security and functionality concerns. These free platforms often have limitations on meeting duration, participant capacity, and advanced security features, which may compromise the integrity of sensitive institutional discussions. For official meetings, conferences, and academic presentations, only licensed and secured platforms, such as Zoom Pro, Microsoft Teams, or other approved enterprise-level services, will be used. This ensures that meetings are conducted with the necessary security protocols, including encryption, password protection, and administrative controls, to safeguard institutional information and maintain a professional environment.

10.2. Subscription on Virtual meeting platform

INES-Ruhengeri should maintain a subscription to secure, enterprise-level virtual meeting platforms for all official meetings, academic sessions, and institutional events. Subscriptions to platforms such as Zoom Pro, Microsoft Teams, or other approved services ensure that meetings are conducted with advanced security features, including end-to-end encryption, password protection, and administrative controls. These platforms also offer extended functionality, such as larger participant capacities, break-out rooms, and robust collaboration tools, which are essential for hosting productive and professional virtual meetings. By subscribing to these secure platforms, the institution can protect sensitive data, ensure compliance with privacy regulations, and facilitate seamless communication across various Departments, stakeholders, and external partners.

10.3. Support of during virtual meeting platform use

The IT Directorate at INES-Ruhengeri is tasked with providing comprehensive support for virtual meeting platforms during all official meetings, academic sessions, and institutional events. This includes assisting with the setup, configuration, and troubleshooting of the platforms to ensure that all meetings run smoothly and securely. The IT Directorate will ensure that meeting links are properly generated, access controls are in place, and technical issues are promptly addressed. Additionally, they will offer guidance on the secure use of these platforms, including user training and ensuring compliance with best practices for data privacy and security. Through their dedicated assistance, the IT Directorate guarantees that virtual meetings at INES-Ruhengeri are conducted efficiently, with minimal disruptions and maximum security.

11. Budget to implement this policy

INES-Ruhengeri must be providing the necessary budget to effectively implement its ICT Policy, ensuring that all technological needs are met for both academic and administrative functions. The budget allocation will cover essential areas such as the acquisition and maintenance of hardware and software, upgrading network infrastructure, and ensuring access to secure virtual meeting platforms. It will also support staff training, security measures, and the continuous improvement of the ICT environment to align with the institute's goals of fostering a modern and innovative educational institution. The funding will be allocated annually and reviewed to adapt to changing technological demands and institutional priorities.

The budget provided for ICT implementation will also ensure the sustainability of the policy over time, enabling INES-Ruhengeri to stay at the forefront of technological advancements. This includes investing in research tools, upgrading the IT infrastructure, and expanding access to online resources and e-learning platforms. The institute recognizes that a robust ICT framework is critical for maintaining high standards of academic delivery and efficient administrative operations.

12. Statement of Enforcement of Policy

(a) The Director, ICT directorate, in liaison with the INES-Ruhengeri Management, ICT Centre Section Heads and the ICT Project Leaders shall be responsible for enforcing these policies and standards and where necessary shall take appropriate remedial measures. The Director of ICT directorate shall monitor the implementation of this policy. This policy shall be enforced and practiced in the entire INES-Ruhengeri.

(b) Failure to comply with these policies shall result in immediate withdrawal of services.

(c) Violation of this policy shall be addressed by appropriate INES-Ruhengeri and national legalmechanisms.

Done at INES-Ruhengeri, on 20th February 2025

INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGERI * INES *

Dr. MAZARATI Jean Baptiste

Chairperson of Governing Body