UNIVERSITY OF RWANDA

Information and Communication Technology (ICT) Policy

Approved by Board of Governors Meeting of 24th February 2016

TABLE OF CONTENTS

INTRODUCTION ... 3

1. General Information ... 3
2. Principles ... 3
3. Objectives ... 3
4. Scope ... 4
5. Enforcement of ICT Policy ... 4
   a. Enforcement ... 4
   b. Violation of ICT Policy ... 4

The Policy ... 5

Section I: Security ... 5

1. SECURITY STANDARDS ... 5
2. PERIMETER SECURITY ... 6
3. INTERNAL SECURITY ... 7

Section II: Network ... 9

Introduction ... 9

A. PASSWORD ... 12
1. Introduction ... 12
2. Purpose ... 12
3. Scope ... 12
4. Policy ... 12
5. Guidelines for password construction ... 13
6. Application Development Standards ... 14
7. Systems administrators and user password standards ... 14
8. Enforcement ... 15
9. Definitions & Terms ... 15

B. ANTI-VIRUS ... 15
1. Introduction ... 15
2. Policy statement ... 15
3. Policy Duration ... 16
4. Policy Exclusions ... 16
5. Email and Virus protection ... 16
6. Prohibited use ... 16

C. WIRELESS ... 17

1. Background 17
2. Scope 17
3. Policy 17
4. Procedures and Guidelines 19
5. Responsible Unit 19
D. HOSTING 19
Definition 19
Policy Statement 20
Contractual requirements: 20
Intellectual property and copyright materials 21
Data availability and records retention 22
Section III: Software 22
A. ACQUISITION 22
B. INSTALLATION 25
Section IV: The World Wide Web 26
1. INTRODUCTION 26
2. POLICY STATEMENT 26
3. UNIVERSITY LOGO AND TITLES 27
4. DEFINITION AND RESPONSIBILITY FOR PUBLISHING ON UR WEB (http://www.ur.ac.rw) 27
5. UR OFFICIAL PAGES 30
6. ISSUES INVOLVED IN PUBLISHING ON THE WWW 31
7. University Policies 32
8. PROCEDURE TO GET AN OFFICIAL WEB PAGE PUBLISHED AT UR 33
9. INTERIM PERIOD 33
Section V: Electronic Collaboration and Information Exchange 34
Email 34
Collaboration 35
Purpose 35
Scope 36
Policy 36
Section VI: Backup, Data Recovery and Archiving 37
Introduction 37
Policy 38

INTRODUCTION

1. General Information

Access to sensitive University information by unauthorized persons could result in legal liability, substantial financial loss, violation of privacy and embarrassment to the University. The Campus network, which connect to the outside world through the Internet, is not isolated from the potential of unauthorized access. With an increasing use of computers and networks on Campuses and with people worldwide having access to the University network, it is important that the University of Rwanda (UR) puts in measures to regulate and protect access to institutional information and data. This policy is maintained on the University's web server and is accessible through the ICT Services pages (intranet.ur.ac.rw and others). The web version of the policy is the definitive version and shall always be the most up to date.

2. Principles

i. The University of Rwanda recognizes that information is an asset and is vital to the academic and economic wellbeing of the institution, and shall therefore create security measures and assign responsibilities to protect this asset from loss, theft, and unauthorized modification or disclosure.

ii. All measures must conform to established University policies and legal requirements.

iii. Every cost effective measure shall be made to ensure confidentiality, integrity, authenticity and availability of information.

iv. It is a priority for all employees at all levels of the University to protect the confidentiality, integrity, and availability of information resources.

3. Objectives

The purpose of the ICT policy is to:

i. Establish direction, procedures and requirements to ensure the appropriate protection of information handled by the University computer resources.

ii. Emphasize the importance of following ICT policy in the various computer environments and the role of staff.

iii. Assign specific responsibilities to ensure policy implementation.

4. Scope

i. The ICT policy applies to all University owned information or data in all forms including electronic and physical.

ii. The ICT policy applies to all permanent, contract and temporary employees, students, contractors, consultants and other workers at the University, including those affiliated with third parties who access the university computer network.

iii. The ICT policy applies equally to networked servers, standalone computers, peripheral equipment, personal computers, laptops and workstations within UR. It also applies to equipment outside of the University network but authorized for access to the university resources. Resources include data, information, software, hardware, facilities and telecommunications.

5. Enforcement of ICT Policy

a. Enforcement

The Office of the Chief Information Officer shall be responsible for enforcing the policy and for any appeals against ICT Centre decisions.

This ICT policy document shall be reviewed every 3 years by ICT Centre, and changes shall be approved by the Board of Governors of the University of Rwanda.

b. Violation of ICT Policy

Sanctions for violation of the ICT Policy may include, but not limited to deactivation of the user's account and prosecution by law enforcement agencies.

If misuse of passwords lead to a violation of policy and compromise of confidential data, employees and students shall normally be subject to disciplinary action, which may include termination of LDAP / Email account.

ICT users who receive unsolicited offensive or inappropriate material electronically should delete it immediately. Offensive or inappropriate material received from people known to the receiver should be deleted immediately and the sender of the material should be asked to refrain from sending such material again. In the event, that a user does not cease sending unsolicited offensive or inappropriate email, disciplinary action shall be taken and shall normally include deactivation of the user account and legal action.

Computer crimes such as computer fraud, hacking and damage to programs and data and introducing and spreading computer viruses shall normally result in legal action.

This ICT policy comprises the following sections:

a) Security
b) Network
c) Software
d) World Wide Web
e) Electonic collaboration and Information Exchange
f) Backup, Data Recovery and Archiving

The Policy

Section I: Security

1. SECURITY STANDARDS

Confidentiality

Confidentiality refers to the University's needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.

Integrity

Integrity refers to the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

Authorization

Authorization refers to whether a particular user, once identified is permitted access to a particular resource.

Access

Access defines rights, privileges, permissions and mechanisms to protect assets from access or loss.

Appropriate use

ICT Systems may be used only for their authorized purposes; that is, to support the research, education, administrative, and other functions of the University of Rwanda. The particular purposes of any ICT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user. Users are entitled to access only those elements of the ICT Systems consistent with their authorization.

2. PERIMETER SECURITY

General

The statements under 'General' apply to all areas within the perimeter security policy.

i. Users shall be granted access to the UR private network by means of network authorization.

ii. ICT Centre may deploy mechanisms that shall track user activity with regard to unauthorized access to ICT systems.

Internet Service Provider (ISP) Router

The University ISP, controls access and security to the ISP router.

Firewall

ICT Centre shall deploy firewalls to protect the University's internal network and ICT systems from unauthorized access.

The firewall section of the policy includes the following:

The University adopts a closed port policy with the requisite authorization being required to open ports for services.

The firewall shall:

i. Be transparent to internal users so that users may perform all allowed network services without undue disruption.

ii. Permit or deny services to specific Internet Protocol (IP) addresses.

iii. Have auditing capability so that user access can be tracked or audited when necessary.

Demilitarized Zone (DMZ)

The DMZ network is a semi-trusted area for all public-facing servers. The UR web servers and any other public access servers shall be assessed against baseline configuration standards to ensure system security before being placed in the DMZ. The DMZ network can be extended beyond the ICT Centre to selected locations provided valid business or academic addresses are judged by the Centre to exist. Servers installed within the extended DMZ need to be secured by the UR unit hosting the servers.

Intrusion Detection Systems

UR shall deploy Intrusion Detection Systems to identify and prevent intrusive or malicious network activity. In addition, operating system, user accounting, and application software audit logging processes shall be enabled on all host and server systems. Audit logs from the various systems shall be regularly monitored and corrective action taken.

Public Access Servers

All public-facing servers shall be secured and hardened as per the best practices of the operating systems' vendors.

Free Linux Servers

All services that are not required shall be disabled. Only secure authentication shall be permitted. Patch Management to secure servers to be carried out as per recommendations for the respective operating systems.

Remote Access

Systems that have access to both modem dial-up and the University network pose a security risk. Modems for dial-up access shall not be allowed on computers or servers, which connect to the University network without authorization of the ICT Centre. Standalone computers with modem connections must be registered with the ICT Centre.

3. INTERNAL SECURITY

Physical Security

This refers to the protection of equipment, and all information and software contained therein, from theft, vandalism and accidental damage. The data centre where most mission-critical servers and communication equipment is held, is a controlled environment with reliable power supplies, adequate climate control, and appropriate secure access.

Equipment located in publicly accessible areas must be secured and must be fastened down with a cable lock system or enclosed in a lockable computer case. The space in which the equipment is located must be locked at all times with restricted access.

Access Control

i. Department Heads must ensure that revised access rights to ICT systems are communicated to the ICT Centre when user access requirements change.
ii. All access requests and changes shall be subject to the ICT Centre change control procedures
iii. Physical access to the data centre and designated equipment are restricted to authorized personnel only.
iv. Remote users who access the University internal network shall require network authorization.

User Accounts

i. Each authorized user on the University network shall be issued with a unique login account commonly known as the network identity (LDAP User Account).
ii. Users are only permitted access to University computers using their unique network identity and no shared logins are permitted.
iii. Dormant network accounts shall initially be locked before permanent removal.

Passwords

i. Procedures regarding use of password and network accounts for the various systems shall be published by the ICT Centre.
ii. Users are required to use passwords to gain access to ICT systems including their desktop computers.

Change Control

i. All computer and communications systems used in production employ a formal change control process whereby changes to the production environment are initiated. The Change Control process is used for all significant changes to software, hardware, communication links and procedures.

Virus Protection

Additional information on virus protection is available in the UR Anti-virus section.

i. All of the University servers and desktop computers must have up to date virus protection software installed.
ii. Virus checking must be done on all files downloaded from external sources, disks or CDs.
iii. Anti-virus software must be updated shortly after a new version is made available.
iv. Certain file types may be prevented access to the University email system as a necessary precaution against email borne viruses.
v. The ICT Centre shall deploy anti-spam procedures to minimize or prevent spam mail from entering the University.

Section II: Network

Introduction

The University of Rwanda (UR) provides network services to a large number and variety of users, including staff, students and external parties. Compromised security for any networked system can have a detrimental impact on other networked systems and even bring down the entire Campus network. The Information and Communication Technology Centre (ICT Centre) is the primary information technology provider on UR's campus, with services for telephony, computing, and networking. The ICT Centre has Campus-wide responsibility to maintain the integrity and security of networked systems and to provide the wiring and cabling infrastructures that support voice, data and video services.

This policy encompasses all systems directly connected to the UR networks and systems on satellite networks that receive network service from the campus backbone. This includes Campus Internet connections, Ethernet connection, Fibre connection and Wireless Networks.

1. Policy Statement

a. Network Traffic

The ICT Centre shall control access to all intra-campus traffic, all inbound and outbound Internet traffic. The Chief Information Officer their designated officer shall determine what Internet traffic shall be permitted. The ICT Centre shall provide oversight to ensure that the traffic limitations are consistent with both the business and academic goals of UR.

b. Network Bandwidth

Bandwidth is the amount of data that can be sent from one computer to another through a network connection in a certain amount of time. Data flow is negatively impacted by a steady increase in users on the network who transfer data above a standard level or size. This increase in users and demand causes contention, slowing down the speed of transfer for everyone.

- The amount of internet bandwidth available to the University will be increased when feasible.
- The ICT centre may prioritise certain types of internet traffic to improve interactive performance.
- ICT centre will implement access control to discourage excessive use of the network so that users do not negatively impact others.

A Service Level Agreement with the ISP must specifically state how much bandwidth the University receives monthly, performance measurements, agreed upon service levels and problem management.

c. Network Servers

All network servers must be registered through the ICT Centre to ensure that any additions or changes to the Network Servers shall not have adverse effects on the network or attached resources.

d. Network Management

i. The Chief Information Officer or their designated officer is authorized to perform a security audit of any UR network device at any time.

ii. The ICT Centre is the primary administrative contact for all network security related activities.

iii. The ICT Centre shall prepare recommendations and guidelines for network and system administrators and shall post them on the ICT Centre web pages. ICT Centre shall publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches.

iv. The ICT Centre shall coordinate investigations into any alleged computer or network security compromises, incidents, and other problems. To ensure that this coordination is effective, the ICT Centre requests that security compromises be reported (Ext 123 or e-mail: ticket@ur.ac.rw).

v. The ICT Centre shall monitor backbone network traffic in real-time to detect unauthorized activity or intrusion attempts.

vi. If scans or network monitoring identifies security vulnerabilities, the cooperation of the system owners and system managers for the systems and the networks shall be required. If the appropriate contact cannot be determined, the relevant management shall be notified. When a security problem (or potential security problem) is identified the ICT Centre shall take steps to disable network access to those systems and devices until the problems have been rectified.

vii. The Chief Information Officer has the right to remove any network segment from the Campus network until problems affecting the network are identified and solved.

2. Procedures and Guidelines

All network users are responsible for understanding this policy and its implications. To obtain more information regarding network security, users may contact the ICT Centre by e-mailing: ticket@ur.ac.rw or visit the frequently asked questions on www.faq.ur.ac.rw

3. Responsible Organization

The Office of the Chief Information Officer shall be responsible for this policy and for any appeals against the ICT Centre decisions relating to the network security. The ICT Centre shall review the policy annually. Within 4 weeks of the review the UR Senior Management Council shall approve changes.

A. PASSWORD

1. Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may compromise the University Campus network. As such, all UR employees, including contractors, vendors and visitors with access to UR systems, are responsible for taking the appropriate steps, outlined below, to select and secure their passwords.

2. Purpose

The purpose of this section of the policy is to establish a standard for creating strong passwords, the protection of those passwords, and the regular renewal of passwords.

3. Scope

The scope of this section of the policy includes all personnel or visitors who are responsible for an account (or any form of access that supports or requires a password) on any UR system, or has access to the UR network, or stores any non-public UR information.

4. Policy

Passwords are used to ensure security and prevent abuse of services; it is advisable that strong passwords are enforced.

a. All system-level passwords (e.g., root, enable, Windows Server admin, Linux Server, application administration accounts) shall be changed every 3 months.

b. All user-level passwords (e.g., LDAP, email, web, desktop computer, etc.) shall be changed in every 60 days.

c. User accounts that have system-level privileges granted through group memberships shall have a unique password from all other accounts held by that user.

d. Passwords shall not be inserted into email messages or other forms of electronic communication.

e. Where SNMP is used, the community strings must be defined as something other than the standard defaults of public, private and system and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMPv2).

f. All user-level and system-level passwords must conform to the guidelines described below.

5. Guidelines for password construction

Strong passwords have the following characteristics:

i. Contain both upper and lower case characters (e.g., a-z, A-Z)

ii. Have digits and punctuation characters as well as letters e.g., 0-9,!@#$%^&*()_+|~=\`{}[]:";'<>?,./)

iii. Are at least eight alphanumeric characters long

iv. Is not a word in any language, slang, dialect and jargon

v. Are not based on personal information such as family names

vi. Passwords should never be written down or stored on-line. Users should try to create passwords that they can easily remember.

Passwords Protection Standards

Do not use the same password for UR accounts as for other non-UR access (e.g. personal ISP account or online banking). Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential UR information.

i. Do not reveal a password over the phone to ANYONE

ii. Do not reveal a password in an email message

iii. Do not talk about a password in front of others

iv. Do not hint at the format of a password (e.g. "my family name")

v. Do not share a password with family members, co-workers or reveal it at any time

vi. If someone demands a password, refer them to this document or have them call someone at the (ICT) Centre.

vii. Do not use the 'Remember Password' feature of applications (e.g. Browsers, Outlook, Netscape, and Messenger)

viii. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile phones, tablets or similar devices) without encryption.

ix. Change passwords every month (except system-level passwords which must be changed at least every three months or according to the system specific procedure).

x. If you think an account or password has been compromised, the incident shall be reported to ICT Centre immediately and change all passwords.

The ICT Centre may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user shall be required to change it.

6. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

a. Should support authentication of individual users, not groups. Should not store passwords in clear text or in any easily reversible form
b. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
c. Should support TACACS+, RADIUS and X.509 with LDAP security retrieval, wherever possible.

7. Systems administrators and user password standards

Wherever possible, the same password shall not be used for various UR access needs. Unique passwords shall be required for the first 6 password changes.

Student passwords: The creation of student login accounts to the network is automated through the SRS system. The initial default password is created randomly by the SRS system. Passwords can be changed through the password change facility on the http://webldap.ur.ac.rw site. Students are strongly encouraged and expected to change their passwords after initial login.

Administrators: Operating Systems and Application support administrators of application systems and servers have to meet more stringent password controls. A minimum of 10 characters that must include a mix of alpha numeric and special symbols are required. The same password is not allowed across systems. The password change interval shall at least be on a 3-monthly (90 days) basis.

8. Enforcement

Employees and students may be subject to disciplinary action, up to and including termination of LDAP / Email account, where weak passwords lead to a violation of policy and compromise confidential data.

9. Definitions & Terms

- Application Systems Administrator Account: any account that is for the administration of an application. (e.g. Oracle database administrator, Pastel administrator, eLearning.)
- Server Administrators Account: any account that has root (SU) privileges on UNIX or GNU LINUX systems or admin or administrator privileges on Windows server systems respectively.

B. ANTI-VIRUS

1. Introduction

The purpose of this policy is to establish requirements, which must be met by all users of computers connected to UR networks to ensure effective virus detection and prevention. This policy outlines how viruses can infect the network, how the ICT Centre tries to prevent and mitigate the effect of infections, and how the network users should respond to a virus if they suspect one has infected the network.

2. Policy statement

a. All computers connected to the UR network must have UR's standard, supported antivirus software installed and scheduled to run at regular intervals.

b. The anti-virus software and the virus pattern files must be kept up-to-date.

c. Virus-infected computers must be removed from the network until they are verified as virus free.

d. Lab Administrators and Managers are responsible for creating procedures that ensure antivirus software is run at regular intervals, and computers are verified as virus-free.

3. Policy Duration

a. This policy is effective from the date of ratification by Senate and shall be in force until official notice is given to the contrary.

4. Policy Exclusions

a. The Chief Information Officer can grant permission for a computer (or operating system) that does not have a virus-protection system to be connected to the network.

5. Email and Virus protection

It is the responsibility of everyone who uses the network to take reasonable measures to protect that network from virus infections.

6. Prohibited use

Users shall not use Internet or e-mail services to view, download, save, receive, or send links to, or material including:

a. Offensive content of any kind, including pornographic material.

b. The promotion of discrimination on the basis of race, gender, origin, age, marital status, sexual orientation, religion, or disability.

c. Threatening, harassing or violent behaviour.

d. Illegal activities.

e. The seeming endorsement of advertising and commercial messages.

f. Messages of a religious, political, or racially offensive nature.

g. Gambling.

h. Sports, entertainment, and job information sites.

i. Personal financial gain, including unsolicited requests for money.

j. Forwarding e-mail chain letters, jokes, or stories.

k. Business-sensitive information.

l. Dispersing corporate data to UR's customers or clients without authorization.

m. Opening files received from the Internet without performing a virus scan.

n. Downloading and installing programs, especially spyware or ad-ware, on the workstation.

o. Or any other material that shall be deemed to be in contravention of principles and core values of UR.

C. WIRELESS

1. Background

This section of the policy provides the structure for a campus-wide solution for the implementation of wireless technology, which includes centralized determination of identity and authentication to ensure the provision of the appropriate levels of security.

To ensure the technical coordination required to provide the best possible wireless network for the University, the ICT Centre shall be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. Other departments may deploy 802.11 or related wireless standards access points, but only provided that such deployment is done in coordination with ICT Centre.

2. Scope

The Wireless section of the Policy provides for the following:

a. The central deployment of wireless access points by ICT Centre based on 802.11 and related wireless standards.

b. The provision of wireless service by ICT Centre for campus departments.

c. The management by ICT Centre of 802.11 and related wireless access points on the UR campus.

3. Policy

a. ICT Centre deployment of wireless access points based on 802.11 and related standards

The University's ICT Centre shall be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. No other departments may deploy 802.11 or related wireless standards wireless access points without coordination with ICT Centre.

b. Provision of wireless service by ICT Centre

The ICT Centre shall offer a standard wireless deployment plan that shall meet the needs of most UR departments wishing to construct and operate departmental wireless services. Departments requiring a different wireless deployment plan may contact the ICT Centre to request them to construct and operate either a standard or, if the spectrum is available for it, premium wireless services. The ICT Centre shall work with departments to accommodate any special needs they may have within the technical constraints of the wireless technology, understanding that all requests may not be technically feasible. The ICT Centre shall provide wireless access points only when it is the most cost effective response to a given scenario and only if it falls within the scope of the ICT Centre responsibility as determined by the Director.

c. Quality of wireless service by ICT Centre

The ICT Centre shall provide the best possible quality of wireless network service, ensure network security and integrity, and minimize the interference between the campus wireless network and other products deployed throughout campus.

d. Coverage of wireless service by ICT Centre

The ICT Centre shall install access points (APs), which shall provide highly reliable network performance and wireless coverage in most campus buildings. The ICT Centre shall monitor wireless use, provide regular reports, and make recommendations to increased coverage in appropriate buildings.

e. Management by the ICT Centre of 802.11 and related wireless standards access points

The ICT Centre shall ensure that all wireless services deployed on campuses shall adhere to campus wide standards for access control. The ICT Centre shall manage the wireless spectrum in a manner that ensures the greatest interoperability and roaming ability for all departments wishing to use wireless technology, and shall centralize the process of determining identity, authentication, and appropriate levels of security for access to and use of wireless technology. The ICT Centre reserves the right to minimize interference to the common wireless network, and shall work with departments to reconfigure or shut down any departmental wireless networks that interfere with the common wireless network.

4. Procedures and Guidelines

The ICT Centre shall advise on wireless plans, deployment strategies, and management issues. Any department wishing to work with the ICT Centre to deploy wireless access must contact the Centre e-mail: (ticket@ur.ac.rw) to begin the process. Departments must also ensure that hardware and software purchased adhere to campus wireless standards.

Departmental wireless networks shall be treated as alliance networks as defined in the Network Security Policy; this requires a formal agreement between the ICT Centre and the department. In the case of existing wireless technology deployments that use the same or interfering spectrums, the ICT Centre shall work with the departments in question to minimize interference to the common wireless network. All sensitive data being transmitted across a wireless network should be encrypted.

5. Responsible Unit

The Office of the Chief Information Officer shall be responsible for this policy and for any appeals against decisions relating to wireless deployments. The ICT Centre shall review the policy annually, and changes shall be authorized by the approval of the Senior Management Council within 4 weeks. The ICT Centre shall review LAN wireless access standards on an annual basis and recommend changes to this policy as needed.

D. HOSTING

The University of Rwanda provides a centrally managed and administered hosting environment that provides solutions for most applications. However, due to capacity and technical considerations the university may opt to host applications externally. This Policy describes the requirements for appropriate and approved use of externally hosted systems and/or data.

Definition

External hosting of systems and/or data can be categorized as the following models:

a) Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

b) Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

c) Infrastructure as a Service (IaaS) is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it.

Policy Statement

- Before systems and data can be hosted externally, a clear and detailed explanation should be provided as why they should not be hosted on the University's internal network.
- For external hosted systems and/or data, the ICT Centre shall ensure that the systems protections are implemented as well as compliance with the ICT policy.
- If sensitive data and/or confidential data are stored on cloud computing services, the relevant contracts must be approved by the Senior Management Council and such system's protections must be assessed by the ICT Centre prior to implementation and reassessed on a periodic basis thereafter, as determined by the level of risk.

In addition to other University policies, the following requirements which must be followed in the use of cloud computing services:

Contractual requirements:

Both the University and vendor must declare the type of data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the data owned by each party. The parties also must clearly define data that must be protected.

The contract must specifically state what data the University owns. Departments must exercise caution when sharing sensitive or confidential within a cloud computing service.

The contract must specify how the vendor can use University Data. Vendors cannot use University data in any way that violates the law or University policies.

Ensure a Service Level Agreement (SLA) with the vendor exists that requires:

- Clear definition of services;
- Agreed upon service levels;
- Performance measurement;
- Problem management;
- Customer duties;
- Disaster recovery;
- Termination of agreement;
- Protection of sensitive information and intellectual property; and
- Definition of vendor versus customer responsibilities, especially pertaining to backups, incident response, and data recovery.

Cloud computing services should not be engaged without developing an exit strategy for disengaging from the vendor and/or service while integrating the service into normal internal business practices and/or business continuity and disaster recovery plans. The University must determine how data would be recovered from the vendor.

A proper risk assessment must be conducted by the ICT Centre prior to any third party hosting or cloud computing service arrangement.

Intellectual property and copyright materials

University of Rwanda's logos, images, and symbols are owned by the University and may not be used or reproduced without permission.

Data availability and records retention

All academic, administrative, or research related data should be retained according to the records retention requirements.

Data should be backed up regularly to ensure that records are available when needed, as many providers assume no responsibility for data recovery of content.

Section III: Software

A. ACQUISITION

1. Policy Acceptances and Authority

UR has endorsed the Software Development Strategy and delegated responsibility for the maintenance and implementation of this policy to the ICT Centre.

2. Backgrounds and Context

ICT Services have moved toward supporting users with a managed and coordinated process, when selection, purchasing or development of software solutions is required. This policy aims to identify the principles on which this can be carried out.

3. Scope

This section of the policy covers administrative systems, web developments and any system that require ongoing support.

It does not include systems that are purely for the delivery of examples for teaching (therefore having a tendency to be disposable) or systems written purely for research.

4. Clarifications and Feedback

Any queries or feedback regarding this policy or its implications should be directed to the ICT Centre on email to ticket@ur.ac.rw

5. Items Covered by this Policy

There shall be a single approval process. User priorities and requirements, including funding provision shall be identified through, at first, a Development Request. Approval via an Investment Appraisal is required.

The introduction of any new system shall be coordinated and project managed by the ICT Centre. Once requirements and business objectives have been defined the default preference order for the sourcing of a solution shall be:

a. Use an existing supported system
b. Modify an existing supported system
c. Buy a new system
d. Buy a new system then adapt if significant functionality is unavailable
e. Develop a customised system

All administrative systems shall be approved or developed or managed or monitored centrally in order to prevent duplication of effort and maximize resource utilization. Existing systems shall be extended, fixed and upgraded where possible rather than source new solutions.

User requests for enhancements shall be managed through a clear change control mechanism.

6. *Software Development and Acquisition Procedure*

The introduction of a new system shall start with the identification of the need. This shall be in the form of a Development Request with generalized information of requirements that should be forwarded to the ICT Centre Director. In the case of a costly and complex system, an outline Investment Appraisal shall be required that should clearly detail why a new system should be introduced, give an indication of the resources required to deliver and how the system shall be supported after introduction.

Priority shall be given to systems, which deliver benefit to the whole University as opposed to purely local solutions. The ICT Centre shall work with the proposer to identify the correct solution starting with checking the availability of a suitable application on the market.

Once a solution has been identified the Development Request or Investment Appraisal shall be updated and submitted for approval consistent with UR procedures.

7. *Software Development Phases*

The software development could follow the following phases and detailed documentation substantiating the following should be provided to the Chief Information Officer:

a. Requirements specification (Requirements Analysis) b. Design c. Implementation (or Coding) d. Integration e. Testing (or Validation) f. Deployment (or Installation) g. Maintenance

8. *Testing Process and Installation*

The software development projects testing should be done by the end-users of the system who are not involved in the software development process. During the testing process the real or live data shall not be provided. In case if it is necessary for the live data then the respective department representative shall feed the real data for testing. Installation of the software should be done in the ICT Centre or designated location as per the instructions from the Chief Information Officer.

9. *Confidentiality*

Any data belonging to UR is not allowed to be taken outside the UR campus either in the form of hardcopy or softcopy by the software developers or consultants. If it is found that the UR data has been taken out of UR without necessary permissions then it shall be considered a crime and it shall be reported to the Police.

10. *Payment Procedures*

a) First Payment (30%)

After Completion of 7.a, 7.b, and 7.c, a formal approval from the Chief Information Officer is needed for the payment.

b) Second Payment (30%)

After Completion of 7.d and 7.e, a formal approval from the Chief Information Officer is needed for the payment.

c) Final Payment (40%)

After Completion of 7.f, the software development team should provide the following in order to get the formal approval from the Chief Information Officer.

i) Detailed test results

ii) Software and code handover

iii) Clear report of existing user details

iv) Administrator rights

v) Manual of the system

vi) Service Level Agreements

B. INSTALLATION

1. Overview

Allowing employees and students to install software on UR computing devices may create conflicting file versions or DLLs that can prevent programs from running. The introduction of malware from infected installation software, unlicensed software which could be discovered in an audit, and programs which can be used to hack the University's network or attacks other networks from our network are examples of the problems that can be introduced when employees install software on UR equipment.

2. Definitions

a. DLL: Dynamically Linked Library. A shared program module used by one or more programs, often installed as part of a program installation. If the current version of a DLL is overwritten by a newer or older version, existing programs that relied upon the original version may cease to function or may not function reliably.

b. Malware: A wide variety of programs created with the explicit intention of performing malicious acts on systems they run on, such as stealing information, hijacking functionality, and attacking other systems.

c. PDA: Personal Digital Assistant. A portable, hand held computing device capable of running software programs. It may connect to host computers or to wired or wireless networks.

d. Smartphone: A cellular phone with qualities of a computer or PDA. It is capable of running software programs and connecting to computer networks.

3. Purpose

To minimize the risk of loss of program functionality, the exposure of sensitive information contained within UR's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

4. Scope

This policy covers all computers, servers, PDAs, smart phones, and other computing devices operating within UR.

5. Policy statements

a. Employees and students may not install software on UR's computing devices operated within the UR network.

b. Software requests must first be approved by the requester's department head and then be made to the ICT Centre in writing or via email.

c. Software must be selected from an approved software list, maintained by the ICT Centre.

d. The ICT Centre shall obtain the software from the requester and track the licenses, test new software for conflict and compatibility, and perform the installation.

6. Enforcement

Any employee or student found in violation of this policy shall normally be subject to disciplinary action, which may lead to restrictions to access rights and for students, expulsion from the University.

Section IV: The World Wide Web

1. INTRODUCTION

UR recognizes that the World Wide Web (WWW) offers many opportunities for promoting the University, both locally and internationally, as well as for information sharing and collaboration. UR encourages students and staff to publish information on its website, but makes a distinction between official University information, and general information posted by employees and students of the University.

Information about UR that is made available via the WWW should be well integrated and of high quality, accuracy and appearance. The website must promote the image of UR as a place of quality and a place to grow'. Contents of all web pages must be consistent with all UR policies and all relevant laws. UR web pages may not provide links to pages outside UR that are in violation of relevant laws or policies.

2. POLICY STATEMENT

The aim of this section of the policy is to ensure that:

a. Staff and students of UR adhere to minimum standards and a coherent framework for academic departments and service sectors for publishing University information on the Web

b. Consistency in the use of the University's logo and title is maintained

c. Well written, visually appealing pages are created, that are easily identifiable as belonging to UR and promote the University's image and mission

d. The image presented on the Web portrays UR as an institution that can present itself effectively through the effective use of the Web as a medium

e. The image presented of UR is a positive one, and that the pages are not misused by the display of inappropriate or illegal material

f. The image is consistent with these guidelines and easily recognizable to the wider higher education community locally and internationally

g. Obligatory items are included and relevant laws and University rules and regulations are obeyed, including copyright laws

h. All content on the website is managed effectively, is accurate, and up to date

3. UNIVERSITY LOGO AND TITLES

a. University Logo

The title University of Rwanda, its logo, and its crest are the property of the University and they, together with the University's address or departmental addresses, should be used in official pages. The University logo enhances the feeling that we all belong to the same organization rather than a collection of separate Colleges, schools, departments or units each going its own way. Only the standard UR titles may be used and should be depicted by using the font Verdana so that they display correctly on all web browsers. The University logo shall not be used on personal home pages.

b. Other Logos

Certain sectors within UR have their own logo(s), which may be used together with the UR logo on official pages emanating from those sectors. However, it should not displace the UR logo.

4. DEFINITION AND RESPONSIBILITY FOR PUBLISHING ON UR WEB (http://www.ur.ac.rw)

To obviate misunderstandings, the role and responsibilities of persons involved in Web publishing at UR are explained. These definitions and responsibilities do not apply to course material, which is made available only via the UR learning management system, but only to information and marketing material about the University as displayed on an information or marketing website such as http://www.ur.ac.rw/.

a. The responsibility of Information and Communication Technology Centre

The ICT Centre shall provide the Internet connectivity needed for the UR Website to be accessible, shall provide and maintain the web server including regular backups and shall manage authoring permissions on said web server via a suitable content management tool. The ICT Centre has no responsibility with regard to the sourcing, creation, design or maintenance of content, although the ICT Centre help desk unit may be contracted, in preference to any other contractor, for this purpose.

b. Content Management

The UR website shall be based on the principle of devolved content management. The content management system shall provide a simple means for owners of content to maintain their own content and reduce dependency on a central authority for allocation of rights. Content management involves the separate roles of Webmaster and content author. It is important to understand that these are roles, not people, and that one person may provide both roles under some circumstances. These roles are outlined below.

i. The Webmaster

The Webmaster has overall coordinating responsibility for the UR website, and holds root content manager status.

The Webmaster:

- Assists departments to design and publish their pages, but does not provide any finance for this purpose
- Assists departments to identify someone within the department who shall be responsible for maintaining accurate and up-to-date content (content manager, content author)
- Assists departments to identify contractors if they wish to have more than the basic website setup, but does not provide any finance for this purpose
- Shall be proactive in helping to ensure that all departments and sections of UR are represented by a Web presence
- Is responsible for creating and maintaining the access rights to second level of content managers.

ii. Content author

A person designated by a School, department, group or section to carry out one or more of the following tasks:

- Manage user rights and folders within the unit's content area
- Write or collect information for publication on official Web pages
- Maintains the content via the website
- Designates and assign rights to one or more other content authors.

There may be a number of content authors in large units. Content authors can create new folders, and assign other users as content authors of those folders, as well as assign users with only page authoring rights. There shall be one or more root content authors, who shall be responsible for the creation of content authors at the next level. Content authors shall be current staff who shall assume this role in addition to their existing duties. Content authors also maintain rights on shared document folders.

The content author in a department is accountable for the information published in the department's pages, and shall ensure that the department's pages comply with the policy requirements of this document and any other requirements that may be specified from time to time by UR management.

There is a clear distinction between those publishing information on behalf of their departments and those wishing to publish information relating to research and/or personal interests. Space shall be made available for individual user's Web pages under the 'Staff' and 'Student' folders for this purpose.

c. *Staff and Student folders*

Content published in staff and student folders shall be consistent with this policy, and may not compromise the image of UR in any way. Misuse of staff and student content folders shall result in loss of privilege and may result in disciplinary action. Student folders shall be automatically audited and removed once a student is no longer registered at UR. Staff and student personal pages shall not display the UR logo. Staff and student authoring rights shall be made available by a departmental content author. Staff folders must be called 'Staff', and student folders must be called 'Student (note the use of the upper case "S") to enable the compilation of all staff and student pages from a single location.

5. UR OFFICIAL PAGES

a. Index page

The index page (usually the entry point) to a particular folder is the page designated as 'index' within the content management system. Index pages should follow the style used on the site in order to preserve the University's corporate identity, except where the index page is a personal page.

b. School or Departmental Pages

School or Departmental Pages are published on the World Wide Web by Schools or Departments of UR in the course of their teaching, administrative and support duties.

c. Personal Pages

Personal pages are used to post personal information regarding a person's job or role within the University, as well as other personal information that the owner may wish to share via the Web in compliance with this policy. Personal Pages may not be used for financial gain.

d. Hosted Pages

At the discretion of the Chief Information Officer acting on behalf of the Management, the University may agree to host World Wide Web pages on its web server on behalf of Learned and Professional Associations and Societies or similar organisations which already make use of UR's servers. There are certain Essential Requirements with which Hosted Pages must comply, including the terms of the agreement.

e. Requirements

Requirements shall apply to everyone, whether creating official or personal pages. There are certain legal and ethical issues as well as those requirements stipulated by UR from time to time with which web content must comply.

f. Pages under construction

Pages under construction may not be posted on the official UR Website. They should be constructed offline and then placed into the content management system for display online. It is also recommended that under construction pages be avoided on all Web servers hosted from UR unless there is a very good reason for doing otherwise.

g. Accessibility to persons with disabilities

UR is committed to ensuring the accessibility of its website for people with disabilities. The ICT Centre will create a Strategic Plan for Web Accessibility outlining how to integrate accessibility throughout web development. This will ensure that when redesigns or updates are planned, accessibility is included from the start of the project. Accessibility is much less costly and time-consuming when tackled at the beginning of a project, rather than the end

6. ISSUES INVOLVED IN PUBLISHING ON THE WWW

The laws that govern what is published in the traditional printed format apply equally to electronic publishing. Some of the more important considerations, including several University rules, regulations and policies, are mentioned here. All should be borne in mind when preparing information for publication on the Web using UR's computing facilities. Anyone in doubt about whether information on their page(s) might contravene any law or University rules, regulations or policies should first seek the advice of the Webmaster before the content is published.

a. Laws

i. Other People's Files and Plagiarism

Reference UR Intellectual Property Policy

ii. Copyright

Reference UR Intellectual Property Policy

iii. Libel

Libel is a civil legal transgression, which may incur substantial financial penalties. The law relating to libel and slander is complicated and therefore easy to contravene through ignorance. Therefore, published facts concerning individuals or organizations must be accurate and verifiable. Views and opinions must not portray their subjects in any way, which could damage their good name or reputation.

iv. Pictures and video

No pictures or videos of people where the individual is identifiable may be placed on a Web page without the express permission of the person(s) in the picture or video. Every individual has a right to privacy and this includes the right to restrict the use of their own image. In addition, the picture or video may be protected by copyright

v. Incitement

Inciting others to break the law, for example incitement to riot, to hack into computers, and to harass another person is a criminal offence punishable by law.

7. University Policies

a. Policies on Discrimination and Harassment

The University rejects racism and sexism and strives to maintain a strong tradition of non-discrimination with regard to race, religion, gender and sexual orientation in the constitution of its student body and in the promotion and selection of its academic and administrative staff. The University strives to provide a safe environment in which all its members are able to reach their full academic or other work potential. The University shall not tolerate any threat or act [including publication of pages on any WWW server in the domain "ur.ac.rw"] that interferes with an individual's performance at work or in study, or that creates an intimidating, hostile or demeaning work or study environment because of an individual's race, gender, beliefs or sexual orientation.

b. Advertising / Private Business

The purpose of providing Internet access to staff and students is to facilitate research and professional activities and aid the employment responsibilities of all our staff. It is not intended for placing or distributing commercial advertising or carrying on any private business, unconnected with a person's work or research at UR.

c. General Computing Regulations

The University has, in addition to what is contained in this policy document, other rules and regulations governing the use of computing facilities on campus; potential Web authors and publishers must read them carefully.

d. Contraventions

Any person misusing University computer resources or contravening a University policy or regulation regarding the use thereof shall normally be subject to the University's disciplinary procedures.

e. Social Media

Principles of integrity, professionalism, privacy and impartiality should be observed by staff and students when posting on social media. In addition, the University Code of Conduct should be observed.

Employees are allowed to associate themselves with the University of Rwanda when posting on social media but they must clearly brand their online posts as personal and purely their own. The University should not be held liable for any repercussions the employees' content may generate.

The Public Relations Officer shall draft and approve University content to be posted on social media affiliated to the University of Rwanda whereas the student Guild President shall be responsible for content related to students.

Content pertaining to sensitive University information (particularly those found within the University of Rwanda's internal networks) should not be shared with the outside online community. Divulging information such as the University's plans, internal operations and legal matters are prohibited and shall normally lead to disciplinary action.

Proper copyright and reference laws should be observed by staff and students when posting on social media.

8. PROCEDURE TO GET AN OFFICIAL WEB PAGE PUBLISHED AT UR

a. Step 1: Please study the Web Publishing Policy and make sure you understand the requirements.

b. Step 2: Procedures may change from time to time, please check the ICT Centre website.

9. INTERIM PERIOD

Existing content shall be converted to the new system as time and resources permit according to a schedule to be published on the ICT Centre website. During the interim period, before this conversion takes place, current procedures and policies shall continue to apply to existing websites and Web pages

Section V: Electronic Collaboration and Information Exchange

The University of Rwanda provides robust communication and collaboration services, including email, and video and voice conferencing to all members of the campus community, enhancing efficiency and effectiveness of collaboration, communications and scheduling.

Email

E-mail is an official communication channel among staff and students within and outside the University of Rwanda. Proper use of e-mail and other electronic communication mechanisms will avoid waste of resources and enable proper communication with target recipients.

The use of University official email has the following advantages:

i. Sustainably keeps the records and back up of work related information

ii. They serve to uphold confidentiality and integrity of work related information

iii. They serve to reduce potential bad practices associated with use of emails in communication (Personal Email Accountability).

iv. They reduce un-necessary use of papers and implied costs with recognition of official emails as a formal University communication medium.

a. Scope

In light of above all University staff should observe the following policy.

Any information that is not legally required to be kept and presented as hard copy e.g. Invoices, Cheques, Receipts, and Delivery Notes, should be shared on official emails or using other appropriate software applications and recognized as a formal communication.

b. Policy

The University's E-mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or origin.

The ICT Centre will make an effort to prevent unsolicited mail or content deemed as undesirable by the University senior management. It is, however, the responsibility of each and every member of the University to ensure that they do not in any way forward any spam mails. Any violation of the rule shall normally result in deactivation of the user account.

c. Publishing contact information

All University offices should publish on their official websites, the relevant contact information including: Names, Picture, Job title, Phone Number, and Official E-mail, Social Media Handle.

d. Use of e-mail clients

For the purpose of increased productivity, it is strongly advised that staff make use of existing mail clients readily available on devices (Outlook, IOS mail, Android mail etc.) known to provide a range of capabilities like auto-calendars, offline access to emails messages, and auto back-up controls.

e. Security Controls

The ICT Centre shall establish and observe secure control and authentication measures for information access, ICT systems, network, developed and tailored to the business environment of the institution.

Electronic communications including communication from other electronic collaboration tools are public records and subject to the provisions of this policy.

Record management of all electronic documents must comply with ICT policies and guidelines on recordkeeping and management of electronic communications.

Collaboration

The University of Rwanda endorses the secure use of web-based collaboration and social media tools to enhance communication, stakeholder outreach collaboration, and information exchange; streamline processes; and foster productivity improvements.

Purpose

This policy provides direction on use of web-based resources and tools to facilitate collaboration, outreach, communication, and information sharing at the University. These web-based collaboration tools include social media such as wikis, blogs, mashups, web feeds (such as Really Simple Syndication (RSS) feeds), and forums (such as Facebook, Twitter, chatrooms), and collaboration tools such as Skype, WebEx and Microsoft SharePoint.

Benefits of Web-based collaboration and social media technologies include:

- Speed – quick dissemination of information;
- Broad reach – vast networks and super-networks of technology and users;
- Targeted reach – a growing number of interest groups represent topics of specific interest;
- Collaboration – both organizations and the public use Web-based tools to network, build relationships, and look for mutually beneficial collaboration opportunities;
- A medium for dialogue – developers often have the access needed to create new applications and to better assess, measure, and use the technology; and
- Expansion of real-time, sensitive communications – helpful for communication during a disaster or emergency situation

Scope

This policy applies to the use of Web-based collaboration tools on any University of Rwanda Internet/Intranet domains or servers as well as any commercial site in which individuals represent the University. The policy applies to all individuals designing, contributing, maintaining, using, or providing oversight of these tools. Individuals include but are not limited to, full-time and part-time employees, contractors, interns, and volunteers who access or contribute content.

Policy

1. The use of Web-based collaboration tools such as social media tools is highly encouraged. Web-based collaboration is intended for information sharing within and outside of the university.

2. UR will promote accessibility of collaboration tools. Where access to social media sites may intrude upon business operations, the CIO may deem it necessary to limit or block access to social media sites for that organization.

3. UR personnel and organizations must exercise sound judgment when utilizing Web-based collaboration tools. The use of Web-based collaboration tools must promote the mission, goals, and objectives of the University. Such use must also be consistent with applicable laws, regulations, and policy, as well as prudent operational, security, and privacy considerations.

4. UR personnel must maximize the quality, objectivity, utility, and integrity of information and services provided to the public. As such, when officially representing the university, UR personnel must reasonably ensure that the agency position on a topic is properly represented in all communications.

5. Web-based collaboration tools established for official UR use must be authorized, monitored, and moderated. As the content owners, each administration, staff office, program office, and facility is responsible for monitoring and maintaining all posted Web content and assuring that the information is accurate and current.

6. UR employees must edit submissions by the public that contain vulgar language, personal attacks of any kind, or offensive comments that target or disparage any individual or group. Further, UR employees will delete comments that:
    a. Are spam
    b. Are clearly off topic
    c. Advocate illegal activity
    d. Promote particular services, products, or political organizations
    e. Infringe on copyrights or trademarks
    f. Contain unauthorized release of UR Sensitive Data
    g. Clearly violate the Privacy Policy
    h. When it becomes necessary to officially contact individuals, UR employees generally shall not use social media outlets as an official mechanism for contacting individuals.

7. While automated collaborative tools present many useful opportunities, their use must not compromise data confidentiality and integrity.

8. All possible steps must be taken to ensure confidentiality, integrity, and availability of information. These steps include, but are not limited to, system redundancy, automated electronic backups, and secure data storage as well as proper and timely data disposal and media sanitization.

Section VI: Backup, Data Recovery and Archiving

Introduction

The purpose of this Section of the policy is to:

a. Safeguard the information assets of the University of Rwanda

b. Prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster

c. Permit timely restoration of information and business processes, should such events occur

d. Manage and secure backup and restoration processes and the media employed in the process.

This policy applies to all servers in the ICT Data and Telephone Centres, including the Network Attached Storage (NAS).

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.

a. Backup retention periods are in contrast to retention periods defined by legal or business requirements.

b. System backups are not meant for the following purposes:

   i. Archiving data for future reference.

   ii. Maintaining a versioned history of data.

Policy

1. Systems shall be backed up according to the schedule below:

a. Data stored on the NAS appliance shall be regularly backed up as follows:

   i. Incremental backup daily (Mon.-Thu.) and data located on-site.

   ii. Full back up monthly (First Fri.) and data located off-site.

   iii. Differential backup weekly on all other Fridays located on-site.

b. Windows Servers (not in DMZ) shall be regularly backed up as follows:

   i. Incremental backup daily (Mon.-Thu.) and data located on-site.

   ii. Full back up monthly (First Fri.) and data located off-site.

   iii. Differential backup weekly on all other Fridays located on-site.

c. Linux Servers shall be regularly backed up as follows:

   i. Incremental backup daily (Mon.-Thu.) and data located on-site.

   ii. Full back up monthly (First Fri.) and data located off-site.

   iii. Differential backup weekly on all other Fridays located on-site.

d. The Backup catalogue Database shall be regularly backed up as followed:

i. Full back up catalogue backup daily (Mon.-Sun.) copied to tape stored onsite.

ii. Weekly (Fri.) copied to tape and stored off-site.

2. **Backup tapes shall be transported and stored as described below:**

   a. Currently all backups shall be written to reusable LTO1, LTO2 and LT03 media with capacity of 100-400 GB uncompressed (200-800 GB compressed) and a transfer rate of 15-60 MB/Sec (native).

   b. Media shall be clearly labelled and stored in a secure area that is accessible only to ICT staff or employees of the contracted secure off-site media-vaulting vendor used by ICT.

   c. During transport or changes of media, media shall not be left unattended.

   d. Daily backups shall be stored on-site in a physically secured fireproof safe located in a building separate from the Data Centre. Daily backups shall minimally be maintained for one month.

   e. Weekly backups shall be stored in a physically secured, off-site media vaulting location maintained by a third party.

      i. Weekly backups shall be maintained minimally for a period of 4 weeks.

      ii. After the period of four weeks has elapsed, the tapes shall be returned to ICT and shall be either re-used or destroyed.

3. **Media shall be retired and disposed of as described below:**

   a. Prior to retirement and disposal, the ICT Centre shall ensure that:

      i. The media no longer contains active backup images

      ii. The media's current or former contents cannot be read or recovered by an unauthorized party.

   b. With all backup media, ICT shall ensure the physical destruction of media prior to disposal.

4. **Backups shall be verified periodically.**

   a. On a daily basis, logged information generated from each backup job shall be reviewed for the following purposes:

      i. To check for and correct errors.

      ii. To monitor the duration of the backup.

      iii. To optimize backup performance where possible.

b. ICT shall identify problems and take corrective action to reduce any risks associated with failed backups.

c. Random test restores shall be done once a week in order to verify that backups have been successful.

d. ICT shall maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

e. Data shall be backed up regularly and stored securely for purposes of data recovery.

f. The ICT Centre has backup policies for backup and restoration procedures.

5. Data Recovery

a. In the event of a catastrophic system failure, off-site backed up data shall be made available to users within 5 working days after the destroyed equipment has been replaced.

b. In the event of a non-catastrophic system failure or user error, on-site backed up data shall be made available to users within 1 working day depending on the amount of data to be restored.

c. The ICT Centre shall produce a Disaster Recovery Plan, which shall outline the emergency recovery of ICT systems.

d. A DRP simulation test shall be conducted at least once a year to test the ICT Centre readiness.

6. Restoration Requests

a. In the event of accidental deletion or corruption of information, requests for restoration of information shall be made to ticket@ur.ac.rw.

7. Responsibilities

a. Backups and Data Recovery – Network Operation Control (NOC) Team

b. Telephone System Backups – Networking Administrator

c. Verification - CIO / Senior IT Operations, with the owners of the data.

Cotton

Professor Philip Cotton,
Vice Chancellor, University of Rwanda

UNIVERSITY OF RWANDA - UR
REPUBULIKA Y'U RWANDA
UBUMWE - UMURIMO - GUKUNDA IGIHUGU