National University of Rwanda
Butare, Huye
Southern Province
Rwanda

Information and Communication Technology Centre (ICT Centre)

ICT Policies – Version 1.0

Approved By:

Joint Senate and Executive Council on 20-08-2010
Board of Directors on 03-09-2010

Responsible Organization Unit

ICT Center

Contents

ICT SECURITY POLICY

1. INTRODUCTION

a. General Information

Access to sensitive university information by unauthorized persons could result in legal liability, substantial financial loss, violation of personal privacy and embarrassment to the university. The campus networks, which connect to the outside world through the Internet, are no longer isolated from the potential of unauthorized access. With an increasing use of computers and networks on campus and with people worldwide having access to the university network, it is important that the National University of Rwanda (NUR) implements controls to protect access to university information and data.

b. Objectives

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

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

iii. Every cost effective measure will 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.

c. Purpose

The purpose of the security 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 security in the various computer environments and the role of staff and students in ensuring that security.

iii. Assign specific responsibilities for the provision of data and information security.

d. Scope

i. This policy applies to all university owned information or data in all forms including electronic or physical.

ii. The 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 security policy applies equally to networked servers, stand alone computers, peripheral equipment, personal computers, laptops or workstations within NUR and equipment outside of the university network but authorized for access to the university resources. Resources include data, information, software, hardware, facilities and telecommunications.

2. RESPONSIBLE ORGANISATIONAL STRUCTURE

The Office of the Director for Information and Communication Technology (ICT) will be responsible for this policy and for any appeals of ICT decisions relating to the security policy. This policy will be reviewed yearly by ICT Center, and authorized changes will be effected through approval of the NUR Management.

3. SECURITY STANDARDS

a. 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.

b. Integrity

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

c. Authorization

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

d. Access

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

e. 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 National 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 ICT Systems that are consistent with their authorization.

4. PERIMETER SECURITY

a. General

The statements under general will apply to all areas within the perimeter security policy.

i. Users will be granted access to the NUR private network by means of network authorization.
ii. ICT Center may deploy mechanisms that will track user activity as regards to unauthorized access to ICT systems

b. Internet Service Provider (ISP) Router

The university ISP, controls access and security to the ISP router. Their security policy restricts the university from gaining any access to the router.

c. Firewall

ICT Center will deploy firewall/s to protect the university internal network and ICT systems from unauthorized access.

The firewall policy includes the following:

i. The University adopts a closed port policy with the requisite authorization being required to open ports for services.
ii. The Firewall/s should be transparent to internal users so that users may perform all allowed network services without undue disruption.
iii. The Firewall/s should permit or deny services to specific Internet Protocol (IP) addresses.
iv. The Firewall/s should have auditing capability so that user access can be tracked or audited when necessary.

d. Demilitarized Zone (DMZ)

The DMZ network is a semi-trusted area for all public-facing servers. The NUR web servers and any other public access servers will 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 needs exist. Servers installed within the extended DMZ needs to be secured by the center hosting the servers.

e. Intrusion Detection Systems

NUR will 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 will be enabled on all host and server systems. Audit logs from the various systems will be regularly monitored and corrective action taken.

f. Public Access Servers

All public-facing servers will be secured and hardened as per the best practices of the operating systems vendors.
Microsoft Servers Hardening of Microsoft Web Servers as per Microsoft recommendations currently available at http://go.microsoft.com/fwlink/?LinkId=14846 or such additional recommendations as made from time to time.

g. Free Linux Servers

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

h. Remote Access

Modems for dial up access will not be allowed on computers or servers, which connect to the University network without the consent of ICT Center. Stand alone computers with modem connections must be registered with ICT Center. Systems that have access to both modem dial up and the university network pose a security risk.

5. INTERNAL SECURITY

a. Physical Security

Physical security refers to the protection of equipment and all information and software contained therein from theft, vandalism and accidental damage. The datacenter 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 that cannot be locked should be fastened down with a cable lock system or enclosed in a lockable computer case.

b. **Access Control**

i. Department Heads must ensure that revised access rights to ICT systems are communicated to ICT center when user access requirements change.

ii. All access requests and changes will be subject to ICT center change control procedures

iii. Physical access to the datacenter and designated equipment are restricted to authorize personnel only.

iv. Remote users for access to the university internal network will require network authorization.

c. User Accounts

i. Each authorized user on the university network will 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 will initially be locked before permanent removal.

d. Passwords

i. Procedures regarding usage of password and network accounts for the various systems will be published by ICT center.

ii. Users are required to use passwords to gain access to ICT systems including their desktop computers.

e. Data Backups

i. Data will be backed up regularly and stored securely for purposes of data recovery purposes.

ii. ICT center has backup policies that outline the backup and restore procedures as is currently used.

f. Disaster Recovery Plan (DRP)

i. The ICT Center will produce a DRP plan, which will outline the recovery of ICT, systems in an emergency.

ii. A DRP simulation test will be conducted at least once a year to test ICT center readiness.

g. Change Control

i. All computer and communications systems used in production employs 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.

h. Virus Protection

Additional information on Virus protection is available in the NUR Anti-Virus policy.

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 CD's.

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 via email as a necessary precaution against email borne viruses.

v. ICT Center will deploy anti-spam procedures to minimize or prevent spam mail from entering the university.

i. Electronic Mail (Email)

i. The Universities 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 national origin.

ii. ICT Center may introduce mechanisms to prevent unsolicited mail or content deemed as undesirable by the university executive.

NETWORK SECURITY POLICY

Introduction

The National University of Rwanda (NUR) provides network services to a large number and variety of users, including staff, students and external constituencies. Compromised security for any networked system can have a detrimental impact on other networked systems and even bring down the entire campus network. Information and Communication Technology Center (ICT Center) is the primary information-technology provider on NUR's campus, with services for telephony, computing, and networking. ICT Center 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 NUR networks and systems on satellite networks that receive network service from the campus backbone. This includes campus Internet connections, 10BaseT, 100BaseT 1000BaseT, subscriber lines and Wireless Networks.

1. Policy

a. Network Traffic

ICT Center will control access to all intra-campus traffic, all inbound and outbound Internet traffic. The ICT Center Director or his/her designee will determine what Internet traffic will be permitted. The ICT Center will provide oversight to ensure that the traffic limitations are consistent with both the business and academic goals of NUR.

b. Network Servers

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

c. Network Management

i. ICT Center or and ICT Center designee is authorized to perform a security audit of any NUR network device at any time.

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

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

iv. ICT Center will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. To ensure that

this coordination is effective, ICT Center requests that security compromises be reported (Ext 123 or e-mail: ticket@ict.nur.ac.rw).

v. ICT Center will 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 will be required. If the appropriate contact cannot be determined, the department's management will be notified. When a security problem (or potential security problem) is identified ICT Center will take steps to disable network access to those systems and/or devices until the problems have been rectified.

vii. In line with this, ICT Center 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 ICT Center by phoning 123 or e-mailing: ticket@ict.nur.ac.rw.

3. Responsible Organization:

The Office of the Director for ICT will be responsible for this policy and for any appeals of ICT Center decisions relating to the network security. This policy will be reviewed yearly by ICT Center, and changes will be authorized by the approval of the NUR Management. ICT Center will review network security best practices on an annual basis and recommend changes to this policy as needed.

PASSWORD POLICY

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 result in the compromise of the National University of Rwanda (NUR) entire campus network. As such, all NUR employees, including contractors, vendors and visitors with access to NUR systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

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

3. Scope

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

4. Policy

a. All system-level passwords (e.g., root, enable, Windows Server admin, Linux Server, application administration accounts, etc.) must be changed on at least a quarterly basis.

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

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

d. Passwords must 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

a. General Password Construction Guidelines

Passwords are used for various purposes at NUR. Some of the more common uses include: elearning login accounts, web accounts, GroupWise email accounts, screen saver protection, Printer/copier device password.

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

Poor, weak passwords have the following characteristics:

i. The password contains less than eight characters
ii. The password is a word found in a dictionary (English or foreign)
iii. The password is a common usage word such as:
   - Names of family, pets, friends, co-workers, fantasy characters, etc.
   - Computer terms and names, commands, sites, companies, hardware, software.
   - Birthdays and other personal information such as addresses and phone numbers.
iv. Word or number patterns like aaabbb, qwerty, 12345, etc.
v. Any of the above spelled backwards.
vi. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

b. 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, jargon, etc…
v. Are not based on personal information, names of family, etc.
vi. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

c. Passwords Protection Standards

Do not use the same password for NUR accounts as for other non-NUR access (e.g., personal ISP account, online banking, etc.). Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential NUR information. Here is a list of "**don'ts**":

i. Don't reveal a password over the phone to ANYONE
ii. Don't reveal a password in an email message
iii. Don't talk about a password in front of others
iv. Don't hint at the format of a password (e.g., "my family name")
v. Don't share a password with family members, co-workers or reveal it while on vacation.

vi. If someone demands a password, refer them to this document or have them call someone in the Information and Communication Technology (ICT) Center.
vii. Do not use the "Remember Password" feature of applications (e.g., Browsers, Outlook, Netscape, and Messenger)
viii. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
ix. Change passwords every month (except system-level passwords which must be changed at least quarterly or as per system specific procedure).
x. If an account or password is suspected to have been compromised, report the incident to ICT CENTER in person and change all passwords.

ICT CENTER or its delegates 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 will 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/or X.509 with LDAP security retrieval, wherever possible.

7. Systems administrators and user password standards

Where possible, don't use the same password for various NUR access needs. For example, select one password for the Application systems and a separate password for Linux systems. Also, select a separate password to be used for an Windows account and a Linux account. Unique passwords will be required for the first 6 password changes.

Linux Users: The Novell password length for logging into the network is set at 8 characters long. Forced password changes are set for a six monthly (180 day) change period. Users are encouraged to change their passwords on a more regular basis.

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.nur.ac.rw** site. Students are strongly encouraged 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 will at least be on a quarterly basis (90 days).

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 of 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 etc.).

Server Administrators - Any account that has root (su) privileges on UNIX or GNU LINUX systems or admin or administrator privileges on Windows server systems respectively.

ANTI-VIRUS POLICY

Introduction

The purpose of this policy is to establish requirements, which must be met by all users of computers connected to NUR networks to ensure effective virus detection and prevention.

1. Policy

a. All computers connected to the NUR network must have NUR'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/Lab Managers are responsible for creating procedures that ensure antivirus software is run at regular intervals, and computers are verified as virus-free.

2. Policy Duration

a. This policy is effective from the underlying date and will be in force until official notice is given to the contrary.

3. Policy Exclusions

a. Permission may be granted by the Director, ICT for a computer (operating system) that does not have a virus-protection system available to be connected to the network.

4. Appendices

Recommended processes to prevent virus problems:

a. Always run the University standard, supported anti-virus software. Contact the ICT Help-Desk (ticket@ict.nur.ac.rw) for help in loading this software.

b. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

c. Delete spam, chain, and other junk email without forwarding.

d. Never download files from unknown or suspicious sources.

e. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

f. Always scan a floppy diskette/flash disk/external hard disk from an unknown source for viruses before using it.

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

h. If lab-testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

i. New viruses are discovered almost every day. Make sure your anti-virus software is up to date.

j. Report any problem in updating the anti-virus patterns to the Help-Desk (ticket@ict.nur.ac.rw) for rectification.

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. This policy outlines how various viruses can infect the network, how the ICT center tries to prevent and/or minimize infections, and how the network users should respond to a virus if they suspect one has infected the network.

6. Prohibited use

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

a. Offensive content of any kind, including pornographic material.
b. Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
c. Threatening or violent behavior.
d. Illegal activities.
e. Commercial messages.
f. Messages of a religious, political, or racial nature.
g. Gambling.
h. Sports, entertainment, and job information and/or sites.
i. Personal financial gain.
j. Forwarding e-mail chain letters, jokes, or stories.
k. Sending business-sensitive information by e-mail or over the Internet.
l. Dispersing corporate data to NUR'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.

7. How viruses can infect a network

There are actually three various types of computer viruses: **true viruses, Trojan horses, and worms.**

True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to the network, the virus can spread throughout the network and may do damage.

A **Trojan horse** is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run.

A **worm** is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

a. Viruses can enter the network in a variety of ways:

i. E-mail-By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect [organization name]'s network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.

ii. Forwarding jokes to friends is a very common vector for email viruses. Whenever you send, reply or forward a message, your email address is included in the message. When the recipient forwards the message to someone else, and they forward it to someone else, your email address can end up on hundreds of pc's. If any one of those pc's gets infected by a virus, they can send a virus to your e-mail address, even though you may never have directly emailed them. The virus will send a copy of itself to any address in their computer, including spam addresses, so now you are getting viruses, and spam. With most new e-mail viruses, there is no way to trace who sent it, because the source address is forged. Be careful who you give your email address to and who you email.

iii. Disk, CD, Zip disk, or other media—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.

iv. Software downloaded from the Internet—Downloading software via the Internet can also be a source of infection. As with other types of

transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

v. Instant messaging attachments—Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

8. How the ICT center prevents and/or minimizes virus infections

a. Removing Emailed program files at the firewall-Most email viruses hide themselves in program files. These types of program files are removed at the firewall, i.e. exe, com, bat. These are the most common types of files to have email viruses, and in the normal workday, an employee has no need of emailing these types of files. If the transfer of these types of files is necessary, please contact the ICT department.

b. Why do we block programs files from Email transmission? A virus can sweep the internet much faster than an Anti Virus vendor can update their software, by preventing these types of files from ever entering our network, we are proactively preventing infection by new viruses that are not detected by anti virus software.

c. Email Server Anti virus-The email server has an anti virus program that scans all messages and removes viruses before the email message gets to the users desktop.

d. Scanning Internet traffic-All Internet traffic coming to and going from our network must pass through NUR servers and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls. Many types of program downloads will be blocked.

e. Running server and workstation antivirus software-All servers run antivirus scanning software. This software scans our file-sharing data stores, looking for suspicious code. Antivirus protection software is also installed on all organization workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.

f. Routinely updating virus definitions—Every morning, the server virus scanning programs check for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed.

g. When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with a server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

9. How to respond to and report a virus

a. Even though all Internet traffic is scanned for viruses and all files on the NUR's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect NUR's network.

b. The ICT staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus-warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

c. As stated, it is the responsibility of all NUR network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

   i. Do not open unexpected e-mail attachments, even from coworkers or someone you know.

d. Never open an e-mail or instant messaging attachment from an unknown or suspicious source.

e. Never download freeware or shareware from the Internet without express permission of the ICT Center.

f. If a file you receive contains macros that you are unsure about, disable the macros.

g. If you receive a suspicious file or e-mail attachment, do not open it. Call NUR's help desk at extension [123] or send email to ticket@ict.nur.ac.rw and inform the support analyst that you have received a suspicious file. The support analyst will explain how to handle the file.

h. If the potentially infected file is on a disk that you have inserted into your computer, the antivirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the help desk at extension [123]. They will instruct you on how to handle the disk.

i. After the support analyst has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus. (If the file was sent via e-mail, the antivirus software running on our e-mail system will automatically send an e-mail message informing the sender of the virus it detected.)

j. If the file is an infected spreadsheet or document that is of critical importance to NUR, the ICT Center will attempt to scan and clean the file. The ICT Center, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on NUR computers.

WIRELESS POLICY

1. Background

This 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.

Wireless in the Local Area Network using the IEEE 802.11 standard is a fast emerging technology. 802.11 wireless technologies are by nature easy to deploy, but highly sensitive to overlapping frequencies. Because of these characteristics, all wireless use must be planned, deployed, and managed in a very careful and centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network.

Current 802.11 wireless technologies deploy a very low power signal in a frequency band divided into only 3 non-overlapping channels. The primary purpose of these channels is not so much to provide separate networks, but to ensure that adjacent access points with slightly overlapping areas of coverage do not interfere with each other. In the normal case, it is necessary to use all three channels in an integrated fashion as a single unified network in order to achieve an optimal design. It is therefore not feasible to allow individuals to install their own access points without centralized coordination, due to the resulting signal interference and greatly degraded performance to the common wireless network.

To ensure the technical coordination required to provide the best possible wireless network for the National University of Rwanda (NUR), the campus' Information and Communication Technology Center (ICT Center) will 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 Center.

2. Scope

The Wireless Policy provides guidelines regarding the following:

a. The central deployment of wireless access points by ICT Center based on 802.11 and related wireless standards;
b. The provision of wireless service by ICT Center for campus departments;
c. The management by ICT Center of 802.11 and related wireless access points on the NUR campus.

3. Policy

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

The National University of Rwanda 's Information & Communication Technology Center (ICT Center) will 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 Center.

b. Provision of wireless service by ICT Center

ICT Center will offer a standard wireless deployment plan that will meet the needs of most NUR departments wishing to construct and operate departmental wireless services. Departments requiring a different wireless deployment plan may contact with ICT Center to have ICT Center construct and operate either a standard or, if the spectrum is available for it, premium wireless services. ICT Center will 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. ICT Center will 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 ICT Center responsibility as determined by the Director.

c. Management by ICT Center of 802.11 and related wireless standards access points

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

4. Procedures and Guidelines

ICT Center will advise on wireless plans, deployment strategies, and management issues. Any department wishing to work with ICT Center to deploy wireless access must contact ICT Center by phoning 123 or e-mailing: ticket@ict.nur.ac.rw to begin the process. Departments must also ensure that hardware and software purchased adhere to campus standards. Departmental wireless networks will be treated as alliance networks as defined in the Network Security Policy; this requires a formal agreement between ICT Center and the department.-----In the case of existing wireless technology deployments that use the same or interfering spectrums, ICT Center will 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 Director for Information and Communication Technology will be responsible for this policy and for any appeals of ICT Center decisions relating to wireless deployments. This policy will be reviewed yearly by ICT Center, and changes will be authorized by the approval of the Management Committee. ICT Center will review LAN wireless access standards on an annual basis and recommend changes to this policy as needed.

SOFTWARE DEVELOPMENT STRATEGY AND POLICY

1. Policy Acceptances and Authority

The NUR Management endorsed the Software Development Strategy and delegated responsibility for the maintenance and implementation of this policy to ICT Center.

2. Scope

This policy supports and underpins the University's Strategies and Plans. It, together with the following other policies, strategies and guidelines, constitutes the ICT Strategy of the University.

The policy specifically includes administrative systems, web developments and any system, which 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.

3. Clarifications and Feedback

Any queries or feedback regarding this policy or its implications should be directed to the ICT Centre on ext: 120 / 123 or email to ticket@ict.nur.ac.rw

This policy is maintained on the University's web server and is accessible through the ICT Services pages. The web version of the policy is the definitive version and will always be the most up to date.

4. Backgrounds and Context

ICT Services has moved toward supporting users with a managed and coordinated process, rather than a fragmented one, when selection, purchasing or development of software solutions is required. This policy aims to identify the principles on which this can be carried out. The policy will support, by adding detail to, the overall ICT Center Strategy.

5. Items Covered by this Policy

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

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

a. Use an existing supported system
b. Modify an existing supported system
c. Buy a new system

d. Buy a new system then modify/adapt if significant functionality is unavailable
e. Develop a custom system

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

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

6. Software Development and Acquisition Procedure

The introduction of a new system will start with the identification of the need. This will be in the form of a Development Request with generalized information of requirements that should be forwarded to the ICT Center Director. In the case of a costly and/or complex system, an outline Investment Appraisal will 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 will be supported after introduction.

Priority will be given to systems, which deliver benefit to the whole university as opposed to purely local solutions. ICT Center in partnership with the proposer will then work 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 will be updated and submitted to the appropriate approving body at the University.

7. Software Development Phases

The software development could follow the following phases and detailed documentation substantiating the following should be provided to the Director, ICT Center.

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 will not be provided. In case if it is necessary for the live data then the respective department representative will feed the real data for testing.

Installation of the software should be done in the ICT center or designated location as per the instructions from the Director of ICT.

9. Confidentiality

Any data belongs to NUR is not allowed to take outside from the NUR campus either in the form of hardcopy or softcopy by the software developers or consultants. If it is found that the NUR data has taken then it will be considered as a crime and it will be complained to the police for criminal action against theft and robbery.

10. Payment Procedures

a. First Payment (30%)
After Completion of 7.a, 7.b, and 7.c, a formal approval from the Director of ICT is needed for the payment.

b. Second Payment (30%)
After Completion of 7.d and 7.e, a formal approval from the Director of ICT is needed for the payment.

c. Final Payment (40%)
After Completion of 7.f, the software development team should provide the following inorder to get the formal approval form the Director, ICT.

i. A detailed test results
ii. Software & code handover
iii. Clear report of existing user details
iv. Administrator rights
v. Manual of the system
vi. Service Level Agreements

SOFTWARE INSTALLATION POLICY

1. Overview

Allowing employees and students to install software on NUR computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which 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 organization's network are examples of the problems that can be introduced when employees install software on NUR equipment.

2. Purpose

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

3. Scope

This policy covers all computers, servers, PDAs, smartphones, and other computing devices operating within NUR.

4. Policy

a. Employees and Students may not install software on NUR's computing devices operated within the NUR network.
b. Software requests must first be approved by the requester's department head and then be made to the Director, ICT center copy to the Help Desk in writing or via email.
c. Software must be selected from an approved software list, maintained by the Information and Communication Technology center, unless no selection on the list meets the requester's need.
d. The ICT center will obtain the software from the requester and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of the computer/equipment from the employee or disabling the access to the computer/equipment if it is a student.

6. 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.

WWW POLICY

1. INTRODUCTION

NUR recognizes that the Worldwide Web (WWW) offers many opportunities for promoting the University, both nationally and internationally, as well as for information sharing and collaboration. NUR therefore allows and encourages students and staff to publish information on its website, but makes a distinction between official University information, and general information provided by employees and students of the University.

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

2. POLICY STATEMENT

The aims of this policy are to ensure that:

a. We, as staff and students of NUR, adhere to minimum standards and a coherent framework for faculties, academic departments and service sectors for publishing University information on the Web;
b. Consistency in the use of the University's crest and title is maintained;
c. Well written, visually appealing pages are created, that they are easily identifiable as belonging to NUR and promote the University's image and mission;
d. The image presented on the Web portrays NUR as an institution that can present itself effectively through the effective use of the Web as a medium;
e. The image presented of NUR 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 nationally 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 CREST AND TITLES

a. University Crest

The title National 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 faculties departments or units each going its own way. Only the standard NUR 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 and crest shall not be used on personal home pages.

b. Other Logos

Certain sectors within NUR, e.g. the Rwanda Development Gateway, and some student organizations, have their own crest(s), which may be used together with the NUR logo on official pages emanating from those sectors. However, it should not displace the NUR crest.

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

To obviate misunderstandings, the role and responsibilities of persons involved in Web publishing at NUR are explained. These definitions and responsibilities do not apply to course material, which is made available only via the NUR 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.nur.ac.rw/.

a. The responsibility of Information and Communication Technology Center

ICT Center will provide the Internet connectivity needed for the NUR Website to be accessible, will provide and maintain the web server including regular backups and will manage authoring permissions on said web server via a suitable content management tool. The Rwanda Development Gateway (RDG) will provide training for content owners as to how to manage and maintain their content. ICT Center has no responsibility with regard to the sourcing, creation, design or maintenance of content, although the ICT Center help desk unit may be contracted, in preference to any other contractor, for this purpose.

b. Content Management

The NUR website will be based on the principle of devolved content management. The content management system will 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 NUR 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 will be responsible for maintaining accurate and up-to-date content (content manager, content author);
- Assists departments identify contractors if they wish to have more than the basic website setup, but does not provide any finance for this purpose;
- Will be proactive in helping to ensure that all departments and sections of NUR are represented by a web presence;
- Is responsible for creating and maintaining the access rights of second level of content managers.

ii. Content author

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

- Manage user rights and folders within the department's content area,
- Write or collects 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 departmental 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 will be one or more root content authors, who will be responsible for the creation of content authors at the next level. Content authors will be current staff who will 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 page/s, and will 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 NUR management.

Please note, 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 will 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 will be consistent with this policy, and may not compromise the image or NUR in any way. Misuse of staff and student content folders will result in loss of privilege and may result in disciplinary action. Student folders will be automatically audited and removed once a student is no longer registered at NUR. Staff and student personal pages shall not display the NUR logo. Staff and student authoring rights will 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. NUR OFFICIAL PAGES

a. Index page

The index page (usually the entry point) to a particular folder is the page designated as "index" with 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. Faculty or Departmental Pages

Faculty or Departmental Pages are published on the World Wide Web by faculties or departments of NUR in the course of their teaching, administrative and support duties.

c. Personal Page/s

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 Director of ICT Center acting on behalf of the Management, the University may agree to host World Wide Web pages on its web server on behalf of Learned / Professional Associations and Societies or similar organisations which already make use of NUR's server(s). There are certain Essential Requirements with which Hosted Pages must comply, including the terms of the agreement.

e. Requirements

Requirements are a "must" for everyone, whether creating official or personal

pages. There are certain legal and ethical issues as well as those requirements stipulated by NUR from time to time with which web content must comply.

f. Pages under construction

Pages under construction may not be posted on the official NUR 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 NUR unless there is a very good reason for doing otherwise.

g. Accessibility to persons with disabilities

Uses the ALT tag with images to include words that replace graphics for people who use text-to-speech. Put text files next to audio files. There are some free web-based services that will help make web pages accessible to people with disabilities. One is Bobby, located at http://www.cast.org/bobby/, and it is recommended that you use it to check your page content for accessibility. It will also find HTML compatibility problems that prevent pages from displaying correctly on different web browsers.

6. GENERAL STRUCTURE AND LAYOUT REQUIREMENTS

This section describes essential information that must be included in Web pages, and provides format, design and style guidelines.

a. GENERAL STRUCTURE

The general structure of the NUR website is determined by the content management system and is hierarchical in nature to promote devolved management of content.

b. LAYOUT OF HOME PAGE

While there are no absolute and rigid requirements for the structure of home pages for faculties and departments, they are advised to consider the following structure for consistency across the site.

i. Banner

Banners should measure x pixels wide x pixels high. Banners should be named banner.jpg, banner.gif or banner.png depending on file type. Banners with these names uploaded to a particular content folder will automatically replace the default NUR banner on the website, so need to be designed accordingly. Of official pages, the NUR logo must appear prominently on the left or right side of the banner, as must the name National University of Rwanda.

ii. Root folder & subfolders

The following information pages should be contained within the top-level folder of a faculty or department:

- Contact: Faculty/department name and address, Inquiries/More Information, etc.
- About: Your faculty / departments mission statement.

The following information may be contained in sub folders. You may create as many folders as needed, but try to keep the number of folders minimal, and ensure that information contained in them is relevant to the name and popup description of the folder.

- Achievements and objectives
- Community involvement
- Programmes offered
- Programme content
- Post Graduate areas of study
- Research activities
- Colour photograph(s) depicting activities provided that such photographs have been optimized for delivery over the web and are not larger than 30kb in file size.
- Any other information deemed relevant

c. REQUIREMENTS

Each content author is responsible for his/her departmental web page(s), including design, writing, accuracy of information, proofreading, abiding by the legal and ethical issues as well as the University's particular requirements listed above, and for keeping the information and links up to date.

i. Essential Information on Official Pages

The banner with required information as noted above; the name of the unit publishing the page (which may appear on the banner); the E-mail address of the person to whom enquiries should be addressed.

ii. Essential Information on Hosted Pages

The name and contact details of the organisation; the name and email address of the content author. The date of the last revision and the disclaimer will be inserted by the content management system automatically so they do not need to be manually entered by the page author.

iii. Disclaimer

The disclaimer must read as follows:

"The views and opinions expressed on this page are strictly those of the page author/owner and may not reflect those of the National University of Rwanda, nor have the contents of this page been approved by the University through any official process."

iv. Each Information Provider must ensure that:

- The information is appropriate and limited to that which is within his/her jurisdiction;
- Information is not duplicated;
- Hypertext links should be provided to the relevant Web pages and site(s);
- The information provided is accurate and up to date;
- The information complies with the legal and University ethical requirements;
- Links are correct and up to date;
- Note:

  When an Information Provider (whether of an Official Page, Hosted Page or Personal Page) no longer wants to publish his/her information, s/he must remove the relevant page/s from the University's Web Server.

d. Format and Design guidelines

Recommendations regarding writing and layout style of pages:

i. Plan carefully how to organise your information and how to point readers to your pages through the page descriptions of the content management system. To make it easy for readers to find the information they are seeking, you may want to build internal links in some of the pages. Most Web users don't want static information or long documents that need scrolling through many screens. Link your information so that readers can navigate through it easily.
ii. Web pages should be well designed and well written. They should be checked for spelling errors and proofread carefully before publishing. It is advisable to use a suitable style manual and to get design and writing help from the Webmaster.
iii. Keep pages simple, and keep readership and medium in mind.
iv. Many people browsing the Web still have monitors, which can display limited colors. Graphics with primary colors work better than those with subtle colors. Remember, the more complex you make your graphics, the longer your pages will take to load. Some readers may choose to switch off the graphics capability of their browsers. All images should be optimized for the best trade-off between size and image quality before uploading them to the server.
v. Provide a way to gather feedback from users by using "mail to" with E-Mail addresses for readers to send comments / enquiries directly from Web pages. Consider setting up "generic" E-mail addresses for this purpose so that pages do not have to be updated when the responsibility is assigned to another person.
vi. Use the standard templates for Official Pages available in the content management system.

7. LEGAL & ETHICAL ISSUES INVOLVED IN PUBLISHING ON THE

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 NUR's computing facilities. Anyone in doubt about whether information in his/her page(s) may contravene any law or University rules, regulations or policies is invited to seek the advice of the Webmaster before the content is published.

a. Laws of the Land

i. Other People's Files / Plagiarism

It is an offence to publish other people's material or files from either printed or electronic publications, or extracts from such materials or files, as if it was your own material (plagiarism) without acknowledgement or permission of the owner of the material. Quotations of a few words may, however, be included provided the author and the work from which the quotation is taken are clearly identified. Plagiarism is, under certain circumstances, an offence punishable by law. The fact that a file is available from your Web area makes it your responsibility to ensure that any necessary permission has been obtained from the owner.

ii. Copyright

In Rwanda, copyright applies to electronic publications in the same way as to printed publications. Material, whether graphic (photographs, cartoons, songs, software, graphics scanned in from published works or other Web pages) or the written word (articles, poetry, etc.), of which some other person owns the copyright, may not be used without that person's permission.

Sometimes payment and/or suitable acknowledgement are required. One should assume that materials on the Web are copyrighted unless a disclaimer or waiver is expressly stated. If copyright is infringed, the owner of the material concerned may take legal action (i.e. claim damages) against the offender. Anyone wanting to include material from another Web page in his/her own page should link to it rather than copy it.

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 and/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 permission of the person(s) in the picture or video. Every individual has a right to privacy, which includes the right to restrict the use of his/her own image. In addition, the picture or video may be protected by copyright

v. **Incitement**

Please note that inciting others to break the law, for example incitement to riot, to hack into computers, to harass another person, etc. is a criminal offence punishable by law. If other people break any law of their own accord, that's their business; if you incite them to do so you are committing an offence, which may be punishable.

8. 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 will not tolerate any threat or act [including publication of pages on any WWW server in the domain "nur.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/research at NUR.

c. General Computing Regulations

The University has, apart from what is contained in this policy document, other rules and regulations governing the use of computing facilities on campus. Intending Web authors/publishers must read them carefully.

d. Contraventions

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

9. PROCEDURE TO GET AN OFFICIAL WEB PAGE PUBLISHED AT NUR

a. Step 1:

Please study This Web Publishing Policy and make sure you understand the requirements.

b. Step 2:

As procedures change from time to time, please check the ICT Center website.

10. INTERIM PERIOD

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

DATA BACKUP POLICY

Introduction

1. The purpose of this policy is as follows:

    a. To safeguard the information assets of National University of Rwanda.

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

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

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

2. This policy applies to all servers in the Information and Communication Technology (ICT) Data and Telephone Centers, including the Network Attached Storage (NAS).

3. 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 will be backed up according to the schedule below:

    a. Data stored on the NAS appliance will be regularly backed up as follows:
        i. Incremental backup daily (Mon.-Thu.) and data located on-site.
        ii. Full backup 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) will be regularly backed up as follows:
        i. Incremental backup daily (Mon.-Thu.) and data located on-site.
        ii. Full backup monthly (First Fri.) and data located off-site.
        iii. Differential backup weekly on all other Fridays located on-site.

    c. Linux Servers will be regularly backed up as follows:
        i. Incremental backup daily (Mon.-Thu.) and data located on-site.
        ii. Full backup monthly (First Fri.) and data located off-site.
        iii. Differential backup weekly on all other Fridays located on-site.

d. The Backup catalog Database will be regularly backed up as followed:
   i. Full Backup catalog backup daily (Mon.-Sun.) copied to tape stored onsite.
   ii. Weekly (Fri.) copied to tape stored off-site.

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

   a. Currently all backups will 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 will be clearly labeled 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 will not be left unattended.

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

   e. Weekly backups will be stored in a physically secured, off-site media vaulting location maintained by a third party.
      i. Weekly backups will be maintained minimally for a period of 4 weeks.
      ii. After the period of four weeks has elapsed, the tapes will be returned to ICT and will be either re-used or destroyed.

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

   a. Prior to retirement and disposal, ICT Center will 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 will ensure the physical destruction of media prior to disposal.

4. Backups will be verified periodically.

   a. On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
      i. To check for and correct errors.
      ii. To monitor the duration of the backup job.
      iii. To optimize backup performance where possible.

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

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

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

5. Data Recovery

a. In the event of a catastrophic system failure, off-site backed up data will 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 will be made available to users within 1 working day. Dependant on the amount of data to be restored.

6. Restoration Requests

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

7. Responsibilities

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

b. Telephone System Backups – Telephone Networking Engineer

c. Verification - Director / Deputy Director ICT, with the owners of the data.