Ndejje University

Ndejje IT Services (NIS)

LABORATORY SECURITY POLICY

Version 1.10

Commencement Date: 1 August 2008

Category: Information and Communication Technology

Table of Contents

Background

0.1 Ndejje University

Ndejje University was first established in 1992 under a different name and ownership. The University acquired its present status in 1995 under the Anglican Diocese of Luweero. It continued operating under this narrow ownership base until 2002 when the ownership base was enlarged to include all the six Church of Uganda Dioceses in the Buganda Region.

0.2 NDEJJE UNIVERSITY Laboratories

The Ndejje University Laboratories are part of the many ICT resource centers of the University. The Laboratories are located at the Kampala Campus, Lady Irene and Main campuses. They are equipped with 100 physically networked computers[1], under a client- sever infrastructure. The computers have full Internet access and this evidently makes the labs more of a portal for users' online academic research purposes. The labs also house other support hardware which includes the respective furniture for the computers, a rack cabinet for the hub system, and the trunkings that support the physical implementation of the network (LAN[2]).

0.3 The Risk Assessment

The Security Level of the Laboratories to date may be ranked at 4, on a scale of 1 to 10, which is low. Access and monitoring of the facility and the services are the factors that greatly undermine the level of security. Software access is a little regulated with limited accounts available for the student users and administrator accounts reserved for the attendants and staff. The labs are technically controlled by the Ndejje IT Services (NIS), the Department that manages ICT in NDEJJE UNIVERSITY.

[1] Literally a conventional computer system (System Unit, monitor, keyboard, mouse)
[2] Local Area Network

Like most IT labs, there are usually various threats associated. With the use of the Internet, and other file sharing and usage, many possible treats are presented. There are also weak points and vulnerabilities which are exposed due to the monitoring and management of the facility. These include some of the following:

(i) Hardware crash due to power fluctuations

(ii) Human (users') error e.g., hardware mishandling

(iii) Both malicious and un-intended damage e.g peripherals thefts,

(iv) LAN cable[1] breakages

(v) Computer viruses and malicious software.

(vi) Absence of fulltime lab attendant, may lead to thefts

(vii) At some point, due to the nature of the courses taught, there may incompetent users, these are especially common with the new learners and they may cause damages.

(viii) The absence of power back-up and stabilization equipment, may lead to software failure and hardware damage.

0.4 **Risk Mitigation**

This risk mitigation method which defines policy hereafter, is based prioritizing, evaluating, and implementing the appropriate risk-reducing controls from the risk assessment process to implement the three major security controls; prevention, detection and recovery. Because the elimination of all risk is close to impossible, *least-cost approach* and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

1.0 The Lab Policy

This document, hereafter referred to as the Lab Policy (or even just the policy), sets up IT security[2] requirements for the Computer labs of NDEJJE UNIVERSITY. The policy document was developed with references to the systematic risk management process, with reference to NIST SP 800-30 (National Institute of Standards and Technology Special Publication 800-30).

Risk management involves three sub-processes: assessment, risk mitigation, and evaluation and assessment. Through these processes, a balance of the operational and economic costs of

[1] Or the different components connected to the cables, like RJ45

[2]

protective measures to achieve gains in mission capability by protecting the IT systems will be made. This developed the policy

2.0 Objectives

The objectives of this Policy are directed towards the following:

- Ensure the protection of confidentiality, integrity and availability of information and assets.
- Ensure users are aware of and fully comply with all the relevant rules.
- Ensure all staff and students understand the need for information and ICT security and their own responsibilities in this respect.
- Defining the operations and mandate of NIS over this Laboratory

The integrity of the Laboratories depends on the security policy which is implemented by the NIS, Laboratory attendants and the Faculties and departments on ground.

2.1 Information technology security elements

Before we visit the policy, we may need to review the elements of a good security policy . These include:

- Confidentiality and Privacy
- Accessibility
- Accountability
- Authentication
- Availability
- Information technology system and network maintenance policy

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.
Access defines rights, privileges, and mechanisms to protect assets from access or loss.
Accountability defines the responsibilities of users, operations staff, and management.
Authentication establishes password and authentication policy.
Availability establishes hours of resource availability, redundancy and recovery, and maintenance downtime periods.
Information technology system and network maintenance describes how both internal and external maintenance people are allowed to handle and access technology.

2.2 The need for information technology security

The University and all members of the University community are obligated to respect and, in many cases, to protect ***confidential*** data. Medical records, student records, certain employment-related records, library use records, attorney-client communications, and certain research and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including faculty and other personnel records, and records relating to the University's business and finances are, as a matter of University policy, treated as confidential.

Systems (hardware and software) designed primarily to store confidential records (such as the Financial Information System and Student Information System and all medical records systems) require enhanced security protections and are controlled ***(strategic)*** systems to which ***access*** is closely monitored. Networks provide connection to records, information, and other networks and also require security protections. The use of University Information Technology assets in other than a manner and for the purpose of which they were intended represents a misallocation of resources and, possibly, a violation of laws and policies.

3.0 Security Categories

This policy applies to the following categories of security:

3.1 ***Computer system and applications security:*** Central processing unit, peripherals, operating system and data.

3.2 ***Physical security:*** The premises occupied by the Information Technology personnel and equipment.

3.3 ***Operational security:*** Environment control, power equipment, operational activities.

3.4 ***Procedural security:*** Established and documented security processes for information technology staff, vendors, management, and individual users.

3.5 ***Network security:*** Communications equipment, personnel, transmission paths, and adjacent areas.

4.0 Scope

For this Policy, information covers any method of information creation or collection, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created. The Policy is however intended for all Laboratory clients including the students and Staff who use the facility to study, teach and access other materials.

It may however be reviewed from time to time, as the need for review may arise.

4.1 **The Implementation**

This policy applies to the entire IT Lab components.

4.1.1 Physical Security

i) As far as practicable, only authorised persons should be admitted to Laboratory.
ii) Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
iii) All Laboratory ICT equipment should be recorded and security-marked.
iv) An inventory of hardware and software must be maintained.
v) Uninterruptible Power Supply (UPS) units are recommended for use on all the Laboratory equipment.
vi) Equipment should be sited to avoid environmental damage.
vii) Do not leave sensitive or personal data desks, flash disks, floppies and any other media with personal information should be handled in a security consient manner.
viii) There shall always be installed a fire alarm, and a lab fire-extinguisher to be used in the event of a fire outbreak.

4.1.2 Systems Security

i) Access Control

a) NIS reserves the right of admission into the lab premises.

b) Access to the computer systems shall be for only users with valid user accounts or access rights

c) All user accounts shall be secured with personal identification methods, like passwords, as the present lab technologies will be

d) All default user accounts on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria of NIS.

e) User accounts, unless otherwise stated, shall be used only by the registered holder.

f) Unauthorized users shall not be allowed to use restricted resources, like servers, without authorized supervision.

ii) Safety Restrictions

a) No eats and drinks and other liquid substances be allowed in the lab.

b) No software and/or hardware installations will be made by users without explicit authority through the lab attendant.

c) Users will not shift any lab equipments, like peripherals hardware, without explicit authority through the lab attendants.

d) The labs will be maintained in a clean state

iii) LAN and Internet Use

a) Computers in the labs shall be networked into an architecture that will be defined by NIS as need may arise.

b) There will be Internet access to all computers on the LAN

c) Intrusion detection tools shall be installed and maintained on all servers and hosts containing data classified as high risk.

d) All connections to the Internet shall go through a properly secured connection point as will be defined by NIS.

e) There will be a firewall installed and maintained by NIS.

f) All traffic into the lab's LAN must go through a well maintained firewall, based at NIS. This traffic should not negatively affect the lab network

4.1.3 Software Policy

i) Software installations, be it from storage media-directly or indirectly connected to a host or from Internet downloads, will be made by qualified personnel or with the supervision of qualified personnel. Qualified personnel will be the lab attendants or course facilitators with the expertise thereof.

ii) NIS will use standard software, including operating systems, as deemed necessary for academic needs.

iii) This software may be changed as need arises.

iv) Each computer system will have an anti-virus software installed, and will be updated regularly

4.1.4 Hardware Policy

i) The lab shall always have enough functional computers ready for use.

ii) Each computer and power hardware shall be protected through uninterruptible power supply (UPS) and other adequate power stabilizers in case of load shading and power surges.

5.0 Responsibilities

5.1 Systems users

a) Users of the ICT systems and data in this Laboratory must comply with the requirements of the Policy.

b) Users are responsible for notifying the NIS of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly Laboratory Attendant.

c) Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

d) Adequate procedures must be established in respect of the ICT security implications.

5.2 NIS

a) NIS shall ensure that the university community is aware of and fully complies with this policy (all associated policies).

b) NIS shall be in charge of all lab requests, noted and forwarded by the general lab authorities (systems administrators, facilities or lab attendants).

c) The administration shall define disciplinary action to any individual found to have violated this policy, with respect to other rules, regulations or policies.

5.3 Lecturers and Staff

a) There will be lecturers and/or facilities to educate and/or train users and/or students on the usage and management of lab resources.

b) Lecturers and/or facilities should be in position to respond or mitigate any attack, and are answerable to any avoidable attack.

c) It will be the responsibility of lecturers and facilitators to report any forms anomalies to relevant authority.

5.4 Systems Administrators

a) There will be an office of a systems administrator who will work in relation to other labs and IT infrastructure in the NIS domain

b) The system administrators will be privileged users and thus will have unlimited access to computer systems in order to carry out their responsibilities. This privilege will be used without breach of the policies defined herein

c) It shall be the responsibility of the system administrator to do the following:

- Ensure the implementation of both technical and none technical articles of this policy in the lab.
- Shall have responsibility over the lab attendants
- Secure the integrity of common-access computers and the data they contain

5.5 Lab Attendants

a) The lab shall have at least have one lab attendant who will be under the supervision of the system administrator, and will be a qualified IT personnel by NIS standards.

b) The lab attendants shall be responsible for the adherence to this policy and any preventive management control against security vulnerabilities.

c) The lab attendant is responsible for controlling lab access. Access to the lab and its' resources will only be granted by the lab attendant as deemed by this policy, and any other university rules and/or regulations.

d) The lab attendants shall be responsible for the daily supervision of the lab will also be responsible for the following:

- Daily and continuous lab checks to ensure that it is in order and that security measures and set policies are being followed.

- Ensuring that lab connections are not unnecessarily interrupted or terminated
- All information about IT resources is documented kept well
- Monitoring of user accounts to ensure that only authorized users have access and lock/remove/delete all those accounts that would no longer be viable to use the system as soon as possible.

Policy Definitions

The following definitions apply to all sections of the ICT Policy Manual:

Appropriate and responsible manner means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University Ethics and Social Justice Commitment Statement; it includes incidental personal use of University facilities and services.

Appropriate use means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University's Guiding Ethical Principles; it includes incidental personal use of University facilities and services.

Authorised web server means a web server that is registered with Ndejje IT Services and approved to publish material on the internet.

Breach means an information security incident that involves users not using Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner.

Business Owner means an authorised University officer or his/her delegate responsible for the management of a work area. A Business Owner authorises access to controlled ICT services.

Business or purpose of the University means an action or requirement which the University needs to have directly performed or met, in order to meet its objectives; or an action or requirement which will facilitate the achievement of the University's objectives.

NIS means Ndejje Information Technology Services.

Controlled ICT service means an ICT service that only allows a user access after successful use of a username and password to authenticate themselves.

Copyrighted content means material for which the copyright for the content is held by a third-party other than the University, eg music, computer software, films, video.

Ndejje communications network means that network of electronic communications equipment identified by Internet Protocol (IP) addresses within the ranges used by the University.

Ndejje URL means a particular set of information on the Internet at a location with a Uniform Resource Locator that refers to a host either within the "ndejjeuniversity.ac.ug" domain or within the IP address ranges used by Ndejje.

Electronic Messaging Services means information technologies used to create, send, forward, receive, store, or print electronic messages.

Electronic Identity means the set of essential information about an individual that is stored electronically by the University.

Electronic Identifier means the value that is used in Ndejje electronic systems to uniquely identify an individual. An electronic identifier is an attribute of the electronic identity.

Electronic Information means any information or recorded, either mechanically, magnetically, or electronically, within Ndejje ICT facilities and services, including data, messages, music, computer software, films, video, etc.

Executive Manager means senior staff who have managerial responsibility for organisational area(s) within the University.

ICT means Information & Communication Technology.

ICTC means Information and Communication Technology Strategy Planning Committee.

Information and Communication Technology (ICT) facilities and services means any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic email systems, internet, intranet and extranet. ICT facilities and services covers all types of ICT facilities owned or leased by the University, ICT services provided by the University and computer equipment owned or leased by users which are used to connect to the University networks and/or the Internet

Incidental personal use means infrequent and minor use of ICT facilities and services that does not: (a) interfere with University business operations; (b) breach any State legislation or University policy; (c) breach an ICT vendor's conditions of use or licence agreement.

Information security incident means any information security event that disrupts the expected standard operation of ICT services and facilities.

Infrastructure means the physical equipment used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals and data that are transmitted.

Malware means software written for malicious purposes such as computer viruses, worms, Trojan horses and spyware programs.

Objectionable material as defined by the State as sexually explicit material (including that involving children), incitement to violence, torture, and bestiality.

Operating System(s) means the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output.

Personal web server means equipment that normally functions as an individual person's desktop workstation that has been configured to publish material at a web URL.

Pornography means sexually explicit material that is not Objectionable material.

Qualified means having formal certification for administration of a relevant web server and its related operating system or evidence of successful completion of training courses and/or self-paced modules pertaining to the web server software and related operating system being used in a particular School or Area, or equivalent experience.

Record means any record, irrespective of format, created or received by an individual or group working on behalf of the University that relates to a business activity of the University and is kept as evidence of such activity.

Restricted material as defined by State, includes any material that a reasonable adult, by reason of the nature of the material, or the nature or extent of references in the material to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.

SEMS means Student Electronic Messaging Service.

Software means a specific use for a computer program, such as for accounts payable or payroll. The term is commonly used in place of the terms "application", "operating system" or "program." Examples of programs and software include pre-packaged productivity software (such as spreadsheets and word processors) and larger, customised packages designed for multiple users (such as e-mail).

Staff member means any person who has been offered and has accepted a contract of employment with Ndejje University.

Student means a person who is admitted to, or enrolled in, a unit, course or program of study approved by Ndejje University, which leads to, or is capable of leading to, an academic award of the University. For the purposes of this definition, the academic awards of the University are as recorded in the List of Academic Awards of Ndejje University of Technology.

Student Electronic Messaging Service or *Student E-mail* means the electronic messaging services provided by the University to students via the University student portal and intranet.

University Associate means a person affiliated with and/or providing services to the University.

URL means Uniform Resource Locator, and defines the global address or location of a particular set of information on the World Wide Web.

University means Ndejje University.

Use of Electronic Messaging Services means to create, send, forward, reply, copy, store, print, or possess electronic messages. For the purpose of this procedure, receipt of an electronic message is excluded from this definition to the extent that the recipient may not have control over the content of the message received.

User means a staff member, student or University Associate of Ndejje University, and includes other persons given limited access to University ICT facilities and services in support of the teaching, learning, research, University-based consultancy, and administrative objectives of the University.

Virus means a particular type of software written for malicious purposes; viruses are part of the "malware" family.

Web server means a computer that publishes electronic information via either the http or https protocols.

World Wide Web means a system of Internet servers that support specially formatted documents. The documents are formatted to support links to other documents, as well as graphics, audio, and video files.

RESPONSIBILITIES	
Policy Manager	Systems Manager
Contact	Systems Manager
Tel : 0772406005	
Email: nvirimoses@ndejjeuniversity.ac.ug	
Review Date	1 July 2011

REVISION HISTORY:

Revision Ref. No.	Approved/ Rescinded	Date	Committee/ Board	Resolution Number	Document Reference
New					
Amended					