Fall 2009

An Investigation Into Rewriting a Security Policy for Loreto College

Paul M. Mwai
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

INFORMATION SECURITY POLICY: AN INVESTIGATION INTO REWRITING THE POLICY FOR LORETO COLLEGE MSONGARI

A THESIS

SUBMITTED ON DECEMBER 14, 2009

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY AND SOFTWARE ENGINEERING

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

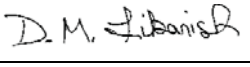
MASTER OF SCIENCE IN SYSTEMS ENGINEERING

By

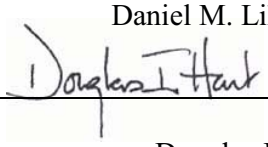
Paul Macharia Mwai

APPROVALS

Robert Bowles, Project Advisor



Daniel M. Likarish



Douglas I. Hart

ABSTRACT

Computers as well as the networking environments in which they operate have evolved into highly sophisticated and complex systems. The intricacy of these systems and especially the relationship between them forms the greatest area of vulnerabilities for organizations. (Whitman and Mattord, 2004)

Information needs to be transmitted to and from the organization, and thus may be vulnerable within certain stages along the communications line. If at any stage of the process, the information is compromised, it could have a negative impact on the entire organization. Protective measures such as disaster recover plans, encryption/ decryption, and information system security controls, can minimize or prevent the negative consequences. Therefore it is vital that management of information system assets take measures to protect their critical data and information from loss damage and misuse.

The process of minimizing risks associated with information security includes the compilation of a detailed and standardized information security policy. Such a policy has to address issues such as threats and possible counter measures as well as defining roles and responsibilities.

The aim of this study was to assess the status of the information security policy compiled and implemented by Loreto College Msongari. During the study, the status of security of the information systems assets at the college, existence and format of the security policy as well as the commitment of the college to address security issues was measured.

ACKNOWLEDGEMENT

It has been an honor to be a part of the Regis University online academic program. It is with great pleasure and relief that I submit this project report as the final requirement to complete the degree requirements

I appreciate all the help and training I received from the various Regis university staff. It was their willingness to share their knowledge and experience that helped me through this project. I would also like to thank Robert Bowles as my advisor, without whom the format and the way forward would never have been formed, and from the degree plan through to the completion of this paper.

Last, but far from least, I would like to thank my family. The constant encouragement from my wife and the endless support from my sons who helped to type parts of this project report. I also know my inspiration played a great role in the completion of this project

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

Loreto College Msongari was founded in early 1990s by the Loreto sisters in Kenya initially to offer secretarial courses, and then information technology courses in collaboration with Jomo Kenyatta University of Agriculture and Technology. The college also offers certification courses such as IT Essentials 1 and CCNA. The college has five computer laboratories with each segment having twenty computers. The staff and the administration have nodes connected to the intranet. Another network segment located in the library has twenty computers. The college population has grown and security threats are increasing day by day. A preliminary survey into the current trend in the use of information technology at Loreto College Msongari suggests that information system assets have become critical to the institution. This is because the college has grown in terms of information technology infrastructure and access to the internet. The college has a duty to preserve and protect these computer information assets.

1.1 Problem Statement

Information security means protecting information system assets from unauthorized access, use, disclosure, disruption, modification or destruction. Appropriate steps must be taken to ensure protection of these vital resources from threats in the form of physical controls, logical controls and administrative controls. The security within any organization starts with building or establishing a security policy. This is a centralized evolving document which defines what is allowed and what is not in the use of information system assets. The policy contains the bylaws of information security for the organization. A security policy needs compliance monitoring and evaluation as the technology evolves to enable its effectiveness in the workplace environments.

This study is concerned with investigating the adequacy of the current security mechanisms in Loreto College Msongari with a view to establishing a security policy that would adequately serve as a guide in the implementation of security controls to the college's information system assets. Therefore, Loreto College Msongari management has found it necessary to mandate the author to review and rewrite the policy to make it more comprehensive and complete in order to mitigate the existing and emerging threats to the college's information system assets.

1.2 Statement of Goals and Objectives

The objective of this study is to establish the current practice of computer security in terms of the level of usage, the knowledge of computer users in the institution in computer security issues, determine the current threats and counter measures and conduct an evaluation of the existing computer network laboratory rules in utilization of the computer resources and documentation with a view to rewriting a security policy in order to establish a security plan that will ensure the protection of confidential and sensitive information stored or transmitted electronically and to ensure protection of the college's information technology resources. The policy will assign responsibilities and provide guidelines to protect the college's information systems and data against misuse and loss.

This security policy will apply to all users of the computer systems, centrally managed information assets, or computers that are authorized to connect to the college's data network such as the internet. It will apply to users of information services operated or administered by the college.

1.3 Significance and Justification

An information system security policy establishes guidelines and standards for accessing the organization's hardware, information and application systems. It informs staff and students of their information protection duties, and tells them what they can and cannot do with respect to the sensitive information.

A policy defines how employees are permitted to represent the organization, what they may disclose publicly, and how they may use organizational computer resources for personal purposes. A clearly defined security policy may be used as a decisive factor in a court of law, showing that the organization took steps to protect its intellectual property.

An information security policy facilitates the communication of security procedures to users and makes them more aware of potential security threats and associated business risks. Thus, it represents a vital element of an organization's information system infrastructure security. With the ever changing varieties of security threats, an accurate inventory of assets, a threat analysis, and classification of risks and how they will be handled is becoming more vital.

1.4 Assumptions of Study

All study participants are assumed qualified to answer questions set forth in the questionnaires. Great care was taken to distribute the right questionnaire to the right random sample of students and employees at all levels. In order for the participants to get clear meaning of the questions, very simple and precise language was used. Some students learn information technology courses and others are in accounting.

1.5 Limitations of the Study

The study, including all background research, interviews, observations and questionnaires was limited to the time between July, 2009 and September, 2009. The participants could not be compelled to participate and notice of the survey could only be distributed via cost free methods. The research is also limited to the college and not the entire Loreto institute.

1.6 Study Methodology

To complete this study, three specific methods were used:

- Reviewing the current data and documentation regarding the existing security policy if any exists. The review includes assessment of threats, the completeness and comprehensiveness of the policy.
- Personal interviews with staff and students and also observations on the operations at Loreto College Msongari.
- A survey of potential risks using questionnaires at Loreto College Msongari.

Chapter 2 - Review of Literature and Research

2.1 Computer Security Concepts

Issues regarding computer security are increasing daily due to advances in technology as well as the global connection of people and resources. Organizations spend large amounts of money on securing their information and information system assets in the quest to stay ahead. An asset is any tangible or intangible thing that has value to an organization. Information system assets include people, data, hardware, network and software.

2.2 Security Concerns

Information need to be protected and preserved in terms of confidentiality, integrity, authenticity, availability and reliability.

The integrity of information is the preservation of information in order to protect the accuracy and completeness of that information and the methods that are used to process and manage it. Information should not be corrupted either deliberately or accidentally.

Availability and reliability is a characteristic that applies to information system asset such that the asset is available if it is accessible and usable when needed by an authorized entity. All of these assets must be available to authorized entities when they need to access or use them. A system should not be tampered with to an extent that a service is no longer available to the users that wish to access it.

Confidentiality ensures that is an information system asset is not disclosed to unauthorized entities. These entities include both individuals and processes. An object should not be revealed to unauthorized individuals.

According to Randy Weaver (2007), computer or cyber crime is becoming more sophisticated because as one weak link or vulnerability is patched; another threat crops up to take its place. Security threats or attacks such as modification of information, interception

of an asset (e.g. eavesdropping), interruption of an asset (e.g. flooding), fabrication of an asset (e.g. counterfeiting or session high jacking), masquerading or denial of service have increased. Fabrication is an attack on authenticity. Attacks are becoming more sophisticated as the computer technology evolves. For instance, viruses and worms spread much faster and cause more damage today than in the past.

According to Bishop (2006), the level and quality of countermeasures to these threats depend on the quality of the security services and the supporting procedures. The mix of these attributes is governed by the security policy of the organization. There are varied definitions of an information system security policy but they all aim at ensuring the protection of information system assets of an organization.

2.3 Common Security Threats

An information system with little or no security is open to a number of threats which may compromise the security concerns stated above. The following are some of the ways in which the computer system can be breached;

● Physical damage in which the physical components of the system are accidentally or maliciously damaged

● Forgery in which an attempt is made to guess or otherwise enable an unauthorized user to breach a security mechanism

● Interception in which an unauthorized user modifies a communication channel unnoticed by communications parties which results in messages being received by an intruder and this leads to loss of privacy.

● masquerading or spoofing in which a third party sends or receives messages uses the identity of another authorized user without delegation of authority. This may lead to breach or loss of integrity, confidentiality and availability.

● Modification in which a message is changed or modified or destroyed accidentally or intentionally. This leads to loss of confidentiality and integrity and may also lead to loss of availability.

● Replay in which a message is first intercepted copied and stored. At a later date it is sent to the recipient. This leads to loss of privacy and may also lead to loss of integrity and availability.

● Repudiation in which a user denies falsely the receipt or sending of a message by the user. Other forms of repudiation include false denial of use, misuse or abuse of resources.

● In-direct infiltration is where an information system is attacked by introducing malicious codes such as viruses, Trojan horse, worm, logic and time bombs. Comprehensive antivirus is widely available to combat this type of attack.

2.4 Security Controls

When management chooses to mitigate or reduce a risk, they will do so by implementing one or more of three different types of controls.

2.4.1 Physical Controls

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For instance; doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, surveillance cameras, alarm systems, barricades, fencing, security guards, picture identification, cable locks, Locked and dead-bolted steel doors and others. They are meant to deter or prevent unauthorized access to the information system assets.

Separating the network and work place into functional areas are also physical controls. An important physical control that is frequently overlooked is the separation of

duties. Separation of duties ensures that an individual cannot complete a critical task all by himself.

2.4.2 Technical or logical Controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform a task.

In general, technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far-reaching in scope and encompass such technologies as: encryption, smart cards, use of backups or replication, network authentication, use of firewalls, intrusion detection and prevention systems, access control lists (ACL) and file integrity auditing software (use of audit trails or log files).

2.4.3 Administrative Controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Examples of administrative controls include the corporate security policy, password policy, hiring policies, disciplinary policies and others.Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what

resources and information by such means as: training and awareness, disaster preparedness and recovery plans, personnel recruitment and separation strategies and personnel registration and accounting. Incidence Response management and the execution of punitive actions are all forms of administrative controls.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance. The main security mechanisms or services which can be employed to meet the demands of a security policy are; authentication, data confidentiality, non-repudiation and administration. They are explained below.

2.4.4 Security Services.

There are various key principles that are followed when controlling access to a computer network as follows;

2.4.4.1 Data confidentiality: this is the process of ensuring that message contents are revealed only to authorized persons. The main technique used here is cryptography. According to Bishop, 2004, cryptography is the science of exchanging secret messages by applying an encryption. Decryption of the cipher text is done using some keys which should not be cracked by an intruder.

2.4.4.2 Authentication: this is the process of establishing proof of identity. A user requires authentication during connection time to access a service. He or she will use passwords. For every message a user needs authentication so that it guards against message replaying and modification. The origin and timeliness of delivery of messages is authenticated.

2.4.4.3 Authorization: this is a process of establishing which users have the right to access an object or service. Once a user is authenticated, access control mechanisms are required to determine which resources the user can access. Access control mechanisms have been

implemented at various levels. For instance, it has been implemented through operating systems and database management software. The most common access control mechanism is to associate each object with an access control list.

A mechanism that blocks message delivery is called a filter. A security fire wall is a set of components which together act as a filter for messages moving in or out of a domain. There are many types of fire walls depending on the scope of action and domain.

2.4.4.4 Non repudiation: this is a process of authenticating the origin of a message to prove or identify the sender. There should be no doubt about the origin of the message. Digital signatures and certificates are used.

2.4.4.5 Security Administration: this is the process of managing the security environment and ensuring that the security policy is enforced and security is not being breached.

2.5 Security Policy Models

A security model entails a comprehensive set of controls comprising the best practices in information security. It is normally an internationally recognized generic information security standard. According to Chow and Mun (2000) standardization within the information technology field is beneficial in that it provides for interoperability and ease of integrating components.

Many organizations exist whose aim is to provide standards and regulations for information system security policy. The National Institute of Standards and Technology (NIST) and International Standards Organization (ISO) are among those organizations that are recognized worldwide as the leaders of security models' formulation. They came up with SP800-x series of documents and ISO 17799 models respectively.

2.5.1 NIST

Information Security Policy

The National institute of standards and technology (NIST) is a non regulatory federal agency within the USA. Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. In terms of computer security it provides principles and practices for securing information security systems. The NIST publications include larger number of documents developed to assist security specialists in designing security frame works. These documents include for instance; the SP 800-12: an introduction to computer security, which focuses on the management of information security and SP 800-14 which: generally gives the acceptable principles and practices for securing information technology system and provides best practices and security principles. Within the document SP 800-14 the first principle for securing information technology systems is the establishment of a sound security policy as the foundation of protecting a system.

2.5.2 ISO17799

This security model entails a comprehensive set of controls comprising best practices in information security, and it is intentionally recognized as a generic information security standard. It consists of ten main sections, namely; security policy, system access control, computer and operations management, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, asset classification and control and business continuity management (disaster recovery plan). Each section contains detailed statements and clauses that comprise the ISO 17799 standard itself as well as provide recommendations for information security management. Critics say that the standard is not as comprehensive as NIST.

2.6 Disaster recovery Plan

As has been said earlier in this chapter, the object of security is to protect valuable and sensitive organization's information and making it readily available. However attackers try to disrupt the normal business operations and steal the information. To achieve their motives and goals, they use various methods, tools and techniques to exploit the vulnerabilities in a computer system or security policy and controls. Security threats can be categorized into mainly human threats and natural threats.

The natural disasters may include; fire, flood, lightning, hurricane, hardware failure due a component or power failure and can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur and damage to the hardware can disrupt other essential services.

Human threats may include; software failure due to bugs, destruction of resources due to vandalism, arson, bombing, cracking, theft, data corruption or loss caused by human errors, media failure such as disks, communications failure, and even industrial action and riots by employees, wars and terrorist attacks.

Few safeguards can be implemented against natural disasters. The best approach is to have a disaster recovery plans and contingency plans in place. Human based threats such as riots, wars and terrorist attacks may be included as disastrous as nothing much can be done about them. Planning and implementation of procedures and facilities for use when essential systems are not available for a period long enough to have a significant impact on the business, e.g. when the head office is blown up.

Organizations need to plan for the type of disasters mentioned above and document the recovery measures to be taken. Preventive measures, recovery and training are very vital in such cases. For instance, hardware can be replaced and is usually insured and can even be replicated. Software and data needs to be backed up frequently off the current site and regularly testing the backups by performing a restore. Alternative communication systems

can be arranged in case of network failure or inaccessible premises, e.g. emergency telephone number, home working, and having an alternative data center.

2.7 Risk Analysis

Security models assist specialists in designing standardized security frameworks. According to Mark Ciampa, the development of a security policy follows a cycle that is never ending. The developer of a security policy needs to identify what needs to be protected, determine how to protect it, and evaluate the protection. The first part of the cycle is risk analysis followed by writing the policy document. Compliance monitoring and evaluation must then be conducted regularly. Information security policy should also relate to the main principles of information security which are confidentiality, integrity and availability.

Risk management plays a critical role in the formulation of protection policy of an organization's information system assets, and therefore its mission, from the information related risk.

2.7.1 Definition

Risk analysis is a technique to identify and assess factors that may jeopardize achieving a goal. The technique helps to define preventive measures to reduce the probability of these factors from occurring and identify the countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the organization. Computer network users and their institutions need to understand what risks exist in their information system assets environment and how those risks can be reduced or even eliminated.

2.7.2 Risk Analysis Steps

The process of risk analysis or assessing and managing risk is as follows;

- Identifying the assets (Knowing what needs to be protected).

- Determining the vulnerability (threat model included integrity, confidentiality and availability).
- Estimating the likelihood of exploitation.
- Documenting the security risks.
- Computing or estimating the cost.
- Surveying and selecting new controls.

Randy (2007) says that those charged with securing systems and the data stored on them must be vigilant. They must also have the support of management and develop a plan to deal with security for their organization. This plan is called a security policy.

2.8 Security Policy

An organization is responsible for its users and other information system assets. Thus, the organization must ensure that a suitable level of controls or counter measures against the attacks is in place and that the adequacy of these safeguards can be demonstrated.

The motivation for an organization to have a security policy may be driven by commercial imperatives, legal requirements or customer demands.

According to Errol Simon (1997), the appropriateness of security services is defined in terms of a set of rules called a security policy. A security policy gives the bench mark against which the security services are measured. The document defines the relevant procedures to security management, the level of responsibility, the reporting needs, and the security mechanisms which must be employed to ensure the enforcement of the security policy.

According to Pfleeger & Pfleeger (2006), a security policy is a high level management document that informs all users of the goals and constraints on using a system, and must answer three questions, namely *who* can access *which* resources in *what* manner. It

defines how employees are permitted to represent the organization, what they may disclose publicly, and how they may use organizational computer resources for personal purposes.

The policy should clearly define the protective measures for these for an organization's information system assets. The existence of a policy defines both the acceptable and unacceptable behavior. For example, spending a lot of time surfing the web and downloading pornography from the Internet are both generally unacceptable. Policies are needed to establish the basis for disciplinary action, up to and including termination.

According to Mark (2005), the backbone of any security infrastructure is its security policy. Without a policy that clearly outlines what needs to be protected, how it should be protected, and what users can and cannot do in support of the policy, there is no effective security in an organization.

This means that the stronger and more comprehensive the security policy is, the stronger the security. Thus a security policy is a critical element in information security.

The need for an information security policy in the strife towards securing of information has been established extensively in both research and industry fields (see Von Solms & Eloff, 2001; Stefanek, 2002; Schneider, 2002; Whitman & Mattord, 2004). However, the question arises on whether they are in existence in organizations and if so, how is their format.

Whitman & Mattord (2005), states that management from all communities of interest must consider security policy as the basis for information security planning, design and deployment. The process of minimizing risks that is associated with information security includes the compilation of a detailed and standardized information security policy. Such a policy has to address issues such as threats and the possible countermeasures as well as defining roles and responsibilities.

Chapter 3 - Research Methodology

A significant portion of this study revolves around generating statistical data regarding not only the status of security threats at the college but also the comprehensiveness and completeness of the current documentation on computer crime and the steps the college may have taken to protect themselves.

3.1 Data type

In this study two questionnaires were designed to capture information on the following aspects that may impact on the security of a computer system or computer environment:

- Use and importance of password
- Physical location of the computer
- Access to the computer
- Records or registers in shared computer environments
- Opinion in computer security in relation to location
- Safety practices in the computer environment
- Awareness on dangers or possible disasters in the computer environment

To capture the information required sample of 61 computer users (students and staff) was drawn randomly from the college population with access to computers. Interviews were conducted at the computer terminals and this was used as a measure of success to the computers. The field data needed to be checked and confirmed to be a true reflection of the interviewee's position. Data was then subjected to descriptive statistical analysis technique of frequency and tabulation analysis.

3.2 Data collection Design

3.2.1 Data Sampling Frame

The sampling frame in this survey is the college and the data elements in this frame are the employees and the students. Loreto College has been selected as a case study because it's an institution where computers play a major role in training and administrative activities.

A working network infrastructure has been in existence since 1999. Computer security is potentially a problem at the college due to network access as well as physical access to the computer locations.

The author's familiarity with the computer systems structure at the college also played a role in the choice of sampling frame.Various organizations and security experts have come up with security frameworks such as NIST model, ISO 177799 model and the basic risk analysis models. These have also been used as a source of data.

3.2.2 Data collection

The primary data has been obtained using questionnaires, personal interviews and observation. The questionnaires targeted staff and students of the college. Computer users were divided into two groups (students and staff or administrators). The collection of data has been conducted at the respondent's place of work. A time frame for the execution of questionnaire has been agreed upon with the respondents as the researcher is a member of staff in the college. The results of questionnaires were cross-checked through visits to the computer rooms and offices.

The results of observation during visitation are recorded and cross-checked with the results of the questionnaires.

The interviews focused on three parts:

- Current practices
- Knowledge on computer security
- Documentation and resources at the college

3.3 Data analysis

The analysis of the data is based on the concepts of physical, logical and administrative controls respectively. The data analysis method applied is the descriptive or summary method.

Graphical and tabulation methods have to a great extent been used because it is easy to understand. MS-Excel spreadsheet package has been used in the data analysis. Note that the human behavior is a relative measure and can only be described using frequency scores. Other information that was used was extracted from reading the literature and internet especially on computer security and other sample security policies.

Choosing the right security model as a guideline to rewriting the security policy is all about what works best for the organization. The researcher considered the culture, the established guiding principles, the challenges the college has experienced in the past and the resources that was available for the policy management function. However, the security policy development cycle has been followed.

The building block for this is risk analysis, security policy formulation or rewriting and finally compliance monitoring and evaluation. The risk analysis was conducted using inspection of the college's existing. Thus, steps such as identification of assets and costing the assets are already documented in the college files. One laboratory consisting of twenty computers has a value of one million Kenya shillings. Loreto College is therefore a medium size organization and it is be easy to conduct participant

Chapter 4 – Project Analysis and Results

The evaluation of the results of this research has been used to draw conclusions on a security policy document for Loreto College Msongari that will contain; the assets to be protected, how each asset is to be protected, who is responsible for protecting each asset and how to respond to security breaches. A security policy is both the baseline for information security in an organization. A policy provides evidence of the organization's position on security and provides a living tool for every employee or student to help build and maintain a certain level of security for the information system assets. It is therefore essential that a security policy be accurate, comprehensive, and useable. The researcher will ensure that the policy document(s) that are produced in this project are as efficient and as useable as possible.

4.1 College network and systems

According to the network administrator and the author's observation, the college has a hundred desktop computers. Ten computers are allocated to the members of staff. The college has only one laptop computer for the principal. The college has four printers. Two of the printers are shareable from the network. The college has two servers running the Linux and Windows 2000 server operating systems. The servers look after the files, the internet connection, e-mail and the student records and accounts database. The internet connection has a 512 Kbps cable modem connection.

The two servers and the desktop computers are linked by 100 Mbps Cat5e Ethernet cables. The college does not have a wireless connection apart from the modem access port. All computers run Windows XP Professional except for the two administrative computers and the eighteen computers in laboratory two which run windows98.

According to the researcher's observation and comparing the network against the checklist in the security guide for small business the following results were found. Computer virus is the greatest threat to the network and yet the antivirus software used is not up-to-date. Most computer users were aware of viruses but were a bit unsure about what they could do to prevent them. Many users complained about spam, but no protection is in place they do not have the knowledge on how to block or filter the spam.

As for the internet connection it was thought that the internet service provider's router included a firewall, but it does not and thus the college does not have one.

All the Windows XP Professional systems are capable of updating the patches through automatically checking and downloading the updates. In Loreto College all the installations of Microsoft Office need updating. The Windows 98 computers are not updated at all.

A random sampling found that most computer users are not using passwords either using easy to guess passwords or had them written on post it notes.

Last year a security company had the alarm system installed so it is pretty good. This was after some desktop computers in offices and laboratories were stolen and they were not insured. It was also difficult to check on their serial numbers due to lack of a log of them.

The researcher also observed that the users share the printers, which means that there is a risk of confidential documents being left there by accident. All the computer users thinks that having fast internet access is a great, but they are using it all the time without much thought to the risks. Also, it was found that most of the web browsing was unrelated to work. Loreto College does not have a policy on acceptable use, and no one is taking any security measures.

The network administrator indicated that back up data on the server is done on a weekly basis, but the restoration of data has not been tested. No user remembers to copy local

files to the server or even to their flash disks. Well-tested backups are essential, as it is to keep a copy of backups off-site.

The researcher through an interview with the network administrator was able to break the risks down into the following four main categories;

- Intruders (viruses, worms, hijacking of our computer resources or Internet connection, and random malicious use). These are the risks that anyone using computers connected to the Internet faces. This is a high risk and it given a high priority.

- External threats (rivals, disgruntled ex-employees, bad guys after money, and thieves). They are likely to use the same tools as hackers, but in deliberately targeting the college and they may also try to induce members of staff to supply confidential information or even use stolen material to blackmail or damage the institution. We need to protect our assets with physical and electronic. This was also ranked as of high risk and high priority.

- Internal threats. Whether accidental or deliberate, a member of staff may misuse his or her privileges to disclose confidential information. This was categorized as of low risk and low priority.

- Accidents and disasters. These are caused by fires, floods, accidental deletions, hardware failures, and computer crashes. They were categorized as low risk and with medium priority. Intruder deterrence should include the implementation of a fire wall, virus protection and strengthening the wireless network.

4.2 Users survey analysis results.

Table 4.1: use of passwords by users of computers at the college

Do you require a password to use a computer?			
		Frequency	Percent
Valid	YES	34	60.7
	NO	18	32.1
	N/A	4	7.1
	Total	56	100

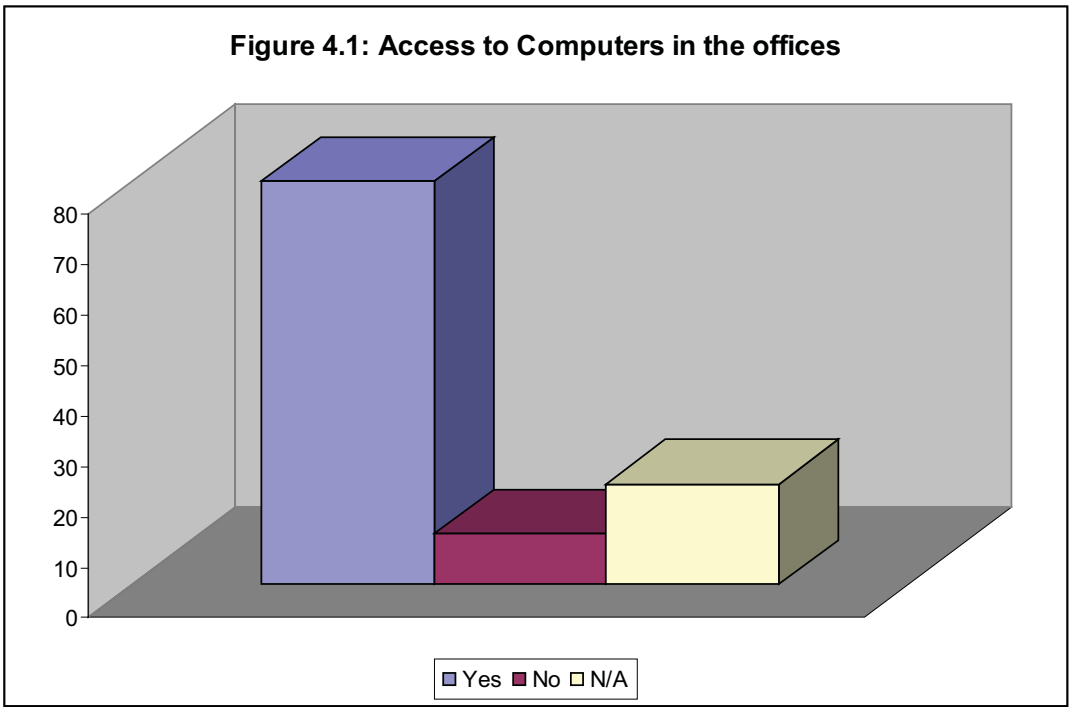
Analysis of the sample data on response of computer users to use of passwords at the college has shown (Table 4.1) that majority use passwords to access the network. That is, 60.7% of the 56 respondents use passwords and only 32.1% do not use passwords. The group that does not use password constitutes a risk in terms of intrusion and therefore threat to the computer systems at the university. The risk percentage requires further investigation. In this survey, the investigation is in the form of perception of users on the use of passwords.

Table 4.2: Perception on the use of passwords as access control

Do you think it is important to use a password to access a computer?			
		Frequency	Percent
Valid	YES	38	67.9
	NO	12	21.4
	N/A	6	10.7
	Total	56	100

A large majority of users, 67.9% of the respondents, considers the use of passwords to control the system access as important. This percentage of user can be offered further training to ensure system security and can understand the need to keep passwords safe. The small percentage that does not value the use of passwords, 21.7%, still constitutes a risk to the security of the computer system. This group of users and the 10.7% that does not constitute relevant information is the vulnerability in the computer system at the college. This requires some physical controls in terms of access like safe rooms and locks.

In this survey, the physical location of the computers accessible to the users is considered relevant to the security of the system. Most computer systems at the Loreto College are located in designated computer rooms, 89%, but 11%, are located in offices for staff. This percentage that is not located in the designated computer rooms is likely to constitute a threat, risk, and vulnerability to computers systems at the college. This is because the computers in the offices are more likely to be accessible to other users in terms of passwords, controls and sharing of resources. Staff share offices and may have common passwords for a shared computer. This therefore calls for analysis of physical access to the computer systems. The results are as in figure 4.1 below, which shows that 64.3% of the computers in offices are accessible to other users and only 14.3% are not accessible to others. This make network or stand-alone vulnerable to intrusion if software controls are not in place.



The shared computer resources often define the entry point of threats to a computer system and define its vulnerability to risk a threat. A good record of computer users must be designed to control access. A slight majority of respondents (57.1%) have indicated that some form of registration exists in terms of access to office computer access. A large portion of respondents, 37.5%, has indicated lack of registration system in access of computers in the offices. This constitutes risk and threats to computer security at the college and is therefore a weak control point. Most users (71.4%) though consider it important to maintain a user register. Implementation of such a system will be tolerable to the users of shared system. The group that does not consider the registration system important can constitute a resistance to the implementation of registration control. Training on the need for access control is necessary for this group of computer users. Information is central in security of computer systems.

Most users, 73.2%, consider the location of computers to be secure and this seems to be what is considered as security by most of them. This supported by the results of password use

data analysis. User generally, 55.4%, do not change their passwords and this, seemingly, is due to the assumption that physical security is adequate. Only 41.1% of the users change their passwords periodically. It is through weak passwords that threats to the computer system occur. Password is of value to the user of the computer only when gaining access to computers but seemingly not a security for the data. Of the 56 respondents, 44.6% think that it's important to change passwords periodically and 39.3% do not think it is useful. seemingly there is no difference in opinion on logging off the work station as the number of users who do not log off, 39.3%, is equal to the number that log off. This means that the main computer system at the college can be vulnerable to intrusion through the number that does not log off the workstation. Threat to data left on the computer screen, is perceived to be real by users, yet logging off is not highly considered. This threat to data is only there if the information is left on the screen otherwise it is not. Users (80.4%) consider leaving work on the screen as harmful may be due to threat of physical loss or plagiarism.

Threat and vulnerability are serious computer security problems but seemingly are not highly regarded. The users seemingly take safety of passwords seriously as majority, 66.1%; do not keep passwords near the workstation. This in itself can be vulnerable as most users may be tempted to use easily traceable passwords. Proper use of passwords of access control should be enforced as most users of the computer tend to value their passwords and do not think sharing of passwords is a good idea. Most users, 83.9%, do not think sharing of passwords is commendable, with only 3.6% in favor. It can therefore be assumed that majority of users will not resist strict implementation of passwords control regime and sharing of passwords is a risk most users would rather do without. There is a tendency by most users, 75% to use passwords of more than four characters. This often requires keeping records of passwords and that the vulnerability, although opinion is divided on the value of lengthy complicated passwords. Of the users included in the sample, 26.8% think it is

advisable to have lengthy passwords and 23.2% do not favor. What is important in the 50% not having a definite opinion on the use of lengthy passwords for they may define the vulnerability of a system at the college?

Table 4.3 below is a measure on the safety of computer data in relation to power availability loss of data when power goes off is one of the security problems faced by computer users. This necessitates use of power back ups as well as regular backup of data. Regular power surge and power loss can lead to permanent loss of data on the computer. There seems to be some power backup for most computers at the university as most users (53.6%) have indicated that their computers remain on when power goes off. It can be said that computer administration considers powers supply stability essential in computer security.

Table 4.3: Power availability and computer use

Does your computer go off immediately power goes off?			
		Frequency	Percent
Valid	YES	17	30.4
	NO	30	53.6
	N/A	9	16.1
	Total	56	100

In terms of computer logical support, there seems to be useful support infrastructure (55.4%) at the college although 32.1% of users have no logical support. This means that logical security problems can be solved in most cases.

One of the most important computer security measures is computer back up. A simple back up is to make copies of the data in the computer. A slight majority of users, 50%, makes copies of their work. This indicates that backup, is not used as security measure but as convenience and portability tool as 40% do not make copies of their work. These users who

backup their work do so regularly, daily to weekly, accounting for 80.6% of the respondents. Even if backup is not used as much as security measures, majorities of users, 78.6%, still view it as important excuse.

Users store their data on flash and compact disks and this is one of the threat points to the computer systems. Portable disks, in terms of security, are a threat because most computer viruses, especially boot viruses, are introduced through use of disks .most users of computers at the college, 62 %, use disks and threat of viruses is therefore real. Portable storage devices are used to copy information from one computer to the other computers. This constitutes potential sabotage threat the college's computer systems. Information stored on the above portable storage devices is vulnerable to physical theft and damage, thus the need to store the disks. The respondents in the sample data tend to store their storage disks near computers (40%) although a sizeable number, 54%, does try to store them away from the computers. The perception here is that there is no need to store the disks away from the computers (49%) this seems to be due to the understanding that the computer rooms or laboratories or offices are safe. The computer users tend to have the basics on the need to backup the data or information and keep it safe but the urgency is lacking.

Lack of urgency, in safe keeping of data is reflected in the disposal printout analysis result. Most users, 48%, reckon that no procedure exists for the disposal of print outs and since this is one of the weak points in access control, the computer at the college are vulnerable to intrusion. This seems to be mainly in cases where computers are in offices and not in designated computer rooms. This means that the college as an institution does not have a set of procedures for the disposal of computer printouts. Despite this problem most users in the sample data, 82%, are aware of the danger of disposing printouts without any caution.

Sharing of computer files is based on the principle of trust and whoever is given access to shared files also has the password. If the access passwords are shared with another

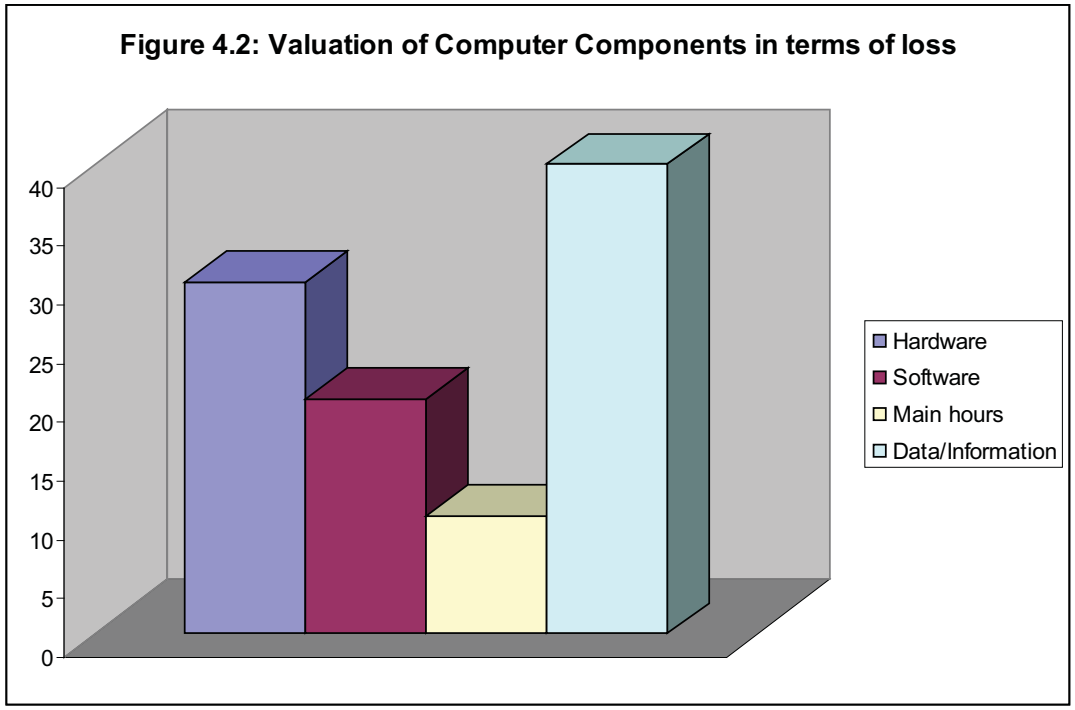
party, then trust principle becomes the weak point in the access control measures. The computer users included in the survey sample, 55% indicated that they shared files with others. Sharing is mainly through swapping computer disks and sharing the same computers. These sharing practices are a threat to the security of both stand alone and network computers, as they are the main entry points of computer viruses as well as intrusions. Making copies of files on disks can also be used to copy restricted files thus the threat of sabotage and espionage. This is usually a threat from insiders and the solution to these problems is usually through persuasion and training but not dismissal of the offenders. A dismissed computer user may turn to be disgruntled and end up being a big threat to the logical and administrative security of the computer system in an organization. Some may even end up being very tricky hackers.

Most users apart from sharing the files have no security access control against unauthorized access. When asked if other users have access to their work, 48% of those in the sample have answered positively and while 36% indicated no.

73% of the respondents indicated that they know that it is harmful to let other people access their work without control. It is not worthy that most users (85.7%) are aware of the danger posed by other users of the computer files in terms of data security. One of the dangers posed by other users of the shared files is that of exposing the contents of an individuals work. For example, 83% of the computer users in the sample are aware of the danger of some one else exposing the content of their work.

A large percentage of the users, 89% , are aware that they can lose their computer equipment if disaster happens but unfortunately, most users consider the physical equipment and software to be collectively important than the data and information. When data or information and man hours are considered collectively, then they rank first ahead of equipment and software. This indicates that the data and information are considered

important only after the physical equipment loss has been assessed. Security is valued more in the college in terms of physical measures.



Most respondents consider storage of data on the computer hard disk a risk, 72%, but the threat and vulnerability of computer systems, are not countered through safe computer security measures.

Data storage on the computer servers is now considered very risky by most users, as 90% have shown that it is a risky practice. In case, it is possible to install stringent access control measures on the use of central computer servers.

The risk of virus infection is viewed as a problem that can be controlled through use of anti virus software. The use of anti-virus is wide spread as 95% of the users have their computers installed with some form of protection software.

96% consider an anti-virus useful as a security measure. The widespread use of anti-virus is seemingly due to the problem posed by viruses to the user, 80% of whom, their work

have been affected. Many users, 75% of the respondents, have lost work on the computers or on their portable storage devices.

The network use at the college is limited but is increasingly becoming part of the computer systems as linking cables get cheaper. The respondents included in the sample survey have indicated that the number of computers linked to the college network especially the internet is less at a time compared with those that are not. Only 20% can access the internet simultaneously. Even though this is the case, the risk in terms of threat and vulnerability, is still high because of sharing of files, disks, and computers. Servicing of computers is not so regular but indications are that logical support is available.

The use of internet is relatively low, but the internet access is mostly used by the respondents to send and receive e-mails (60%). Literature review in chapter two has shown that, opening of junk e-mails or spam is one of the worst mistakes a user can make in terms of virus infection and password security-mails are the main sources of virus infections as well as entry points for back door installation and are therefore both a threat as well as vulnerability in terms of computer system security.

Users need to be trained on the safe use of e-mail services on the internet. Password access is not safe proof security measure on the internet so long as the communication ports of a system are not protected. Actually, there is nothing like ultimate data security when the computer system is connected to the internet. Security measures on the internet should make as hard as possible for intruders to gain access to computer system communication ports and some computer systems in the organization should be completely out of the internet connection.

The researcher found that 80% of the college computer users do downloads on the internet. Internet downloads are the main sources of virus infection, back door implants, and data access. Thus, most computer users at the college who have access to the internet are at

the risk of data security, the problem of un-authorized access to their data files and virus infection.

Table 4.4: Internet access by users

Q42. Do you access the internet?			
		Frequency	Percent
Valid	YES	29	53.7
	NO	25	46.3
	N/A	2	3.6
	Total	56	100

Users of computers, are largely aware of the danger of using internet downloads, 46% but sizeable percentage, 33%, do not think it is harmful to use downloads. This is the risk group of computer user that poses a threat to the computer system security.

The types of operating system and application software affect the level of computer system vulnerability to risk and threat. Most Microsoft operating system and application software are more vulnerable than the UNIX and Linux operating systems. Most computer users, 62%, have Ms Windows XP, therefore constituting 89% of the respondents. Ms operating systems are easier to use and readily available thus their prevalence. Ease of use makes it easier for hackers to access control information for communication port access.

Application software in use is mostly Ms Word, which 80% of the users have followed, by word perfect, 14.3%. Spreadsheet software and database software in use are mainly those of Microsoft. Generally, over reliance on Ms Soft ware by users makes the college computer network very vulnerable.

In conclusion, from the frequency analysis of the users of the data, computer security problems at the college can be summarized as follows:

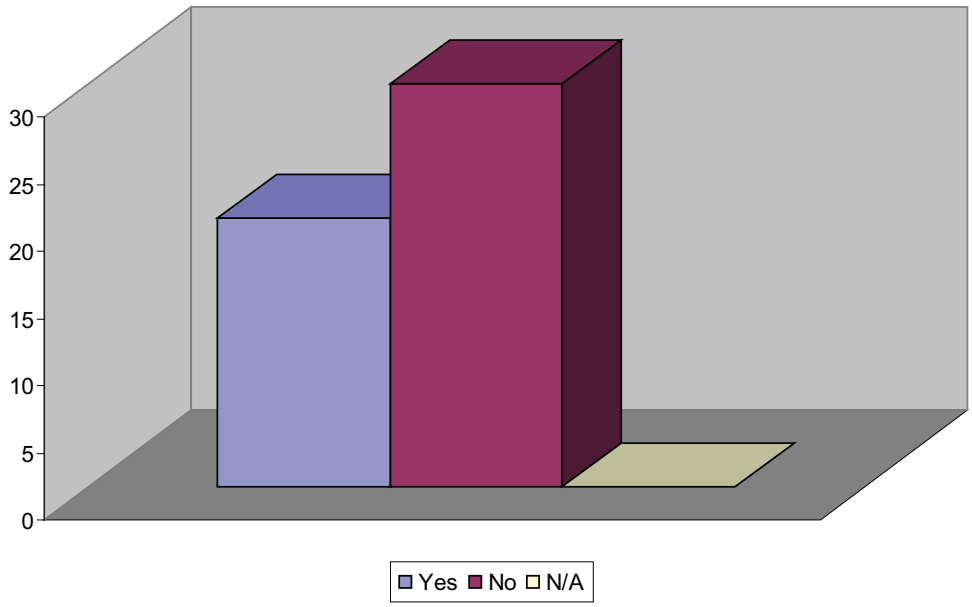
- Lack of proper physical security in terms of access to computers in the offices
- Lack of proper guidelines in password use of and security
- Increased vulnerability to virus infection and back door access due to increased use of internet
- Over reliance on Microsoft operating and application software which are written in Visual Basic and thus are not patched up properly.

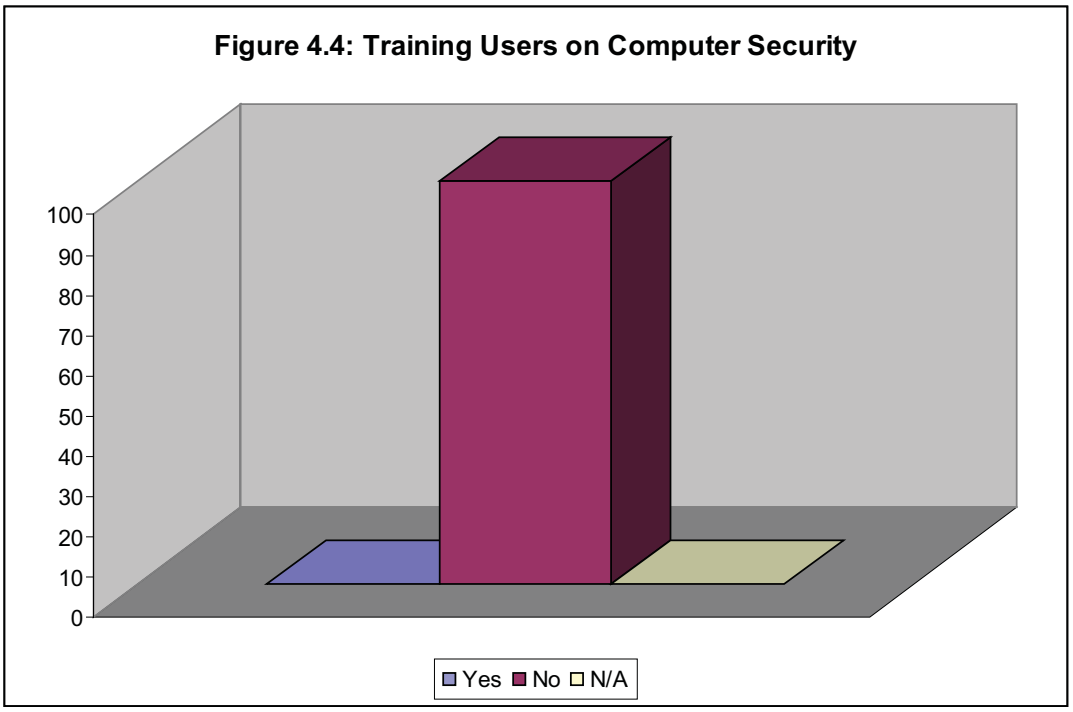
4.3 Analysis results for system administrators' data

4.3.1 Training in computer security issues.

A total number of five system administrators at the college have been included in the sample survey. Most system administrators, 60.0%, the College have not had any formal training in computer security. This indicates that, the concept of security is tending not to be considered crucial issue. That is, so long as one is trained in system administration, he or she can be a system administrator. It is not only the running of the computer system that is important but also the security of information, integrity of data, and physical security.

Figure 4.3: Level of Formal Training on Computer Security





The percentage that has undergone some training (60.0%). 100%of the administrators train users on security issues. That is, those who have been trained in computer security conduct no formal training on computer security. It seems, therefore, that security is not a central characteristic of computer system at the College. Security risk, threat and vulnerability are, seemingly, real problem in the College security system. There is need for agent to be taken in terms of training in security of computer systems.

4.2.2 Documentation on Security Measures

40.0% of systems administrators have put in place some documentation but the majority, 60.0%, has no documentation. This seems to reflect the distribution of training on computer security. It seems that those who have undergone some training in computer security are likely to have in place documentation while those without training are less likely. Since those who have not undergone training is more than the trained and the trained are less likely to train others, security measures are likely to be compromised. This further call for training of system administrators in security matters for it seems that only those with the right training

are likely to take the issue of security measures documentation. Lack of documentation on security matters makes the computer system vulnerable to security breaches and intrusion.

Table 4.5: Use of documentation in Security Control

Q3: Do you have documentation on computer security issues for users?			
		frequency	percent
valid	YES	2	40.0
	NO	3	60.0
	TOTAL	5	100

All system administrators seemingly value some form of documentation on security measures but lack of training may affect the know how on security issues and therefore what to document. Those who have had some training on computer security need to train other system administrators on the need for documentation and what to document. This makes the case for further training for system administrators at the college are an important matter to be addressed by the college administration.

Table 4.6: Opinion in use of documentation as a security control measures

Q4: Do you think documentation and training play a major role in preserving security of our computer resources?			
		frequency	percent
valid	YES	0	0.0
	NO	5	100.0
	TOTAL	5	100.0

4.3.3 Computer Systems access and availability

It seems that the computer administrators at the college do not have a clear idea on the number of computer at the college. They tend to give various answers ranging 60 to 100 with the range 100 to 150 being the most common, 60.0%. This situation suggests that without knowledge of the number of computers at the college, system administrators cannot protect the computers adequately even if they have training in computer security. This is especially so in terms of threat in the form of unauthorized intrusion. Any person with access to a computer terminal or pc, which is linked d to the College network, can interfere with other connected computers. It is important that system administrators have exact knowledge of the number of computers available in the university and what they are used for and who has access to them. Knowledge is the best security for a computer system. And one must be prepared for attack from any quarter and in any form.

Lack of exact knowledge on number of email users makes the college computer systems to be vulnerable to intrusion and risk. One of the main entry points in network intrusion and threats is through email. Email users have access to communication ports and it's through this port that backdoors can be planted thus access to your data file and vulnerability to espionage, virus attack, and system incapacitation. Exact knowledge on number of email users is required for it give indication on the number of those who may have access to the system.

Table 4.7: Knowledge on the number of email users

Q5A: How many users of email do we have at college?			
		frequency	percent
valid	Below 60	0	0.0
	60 - 100	2	40.0
	100 - 150	3	60.0
	200 - 300	0	0.0
	TOTAL	5	100.0

Table 4.8 Knowledge on the number of computers

Q5B: To the best of your knowledge, how many computer servers do we have in college?			
		frequency	percent
valid	1-5	4	80.0
	6-10	1	20.0
	Above 10	0	0.0
	TOTAL	5	100.0

Most serious is the lack of exact knowledge on the number of computer servers at the college. A system administrator must have exact information on the number of servers, as this is important to both administrative and logical security issues. Majority of system administrators, 80.0%, tend to indicate a number ranging from 1-5. This percentage seems to be equal to the percentage that has undertaken training on computer security. Seemingly, a system administrator is likely to pay attention too the number of stand alone, servers and main frames in an organization than those without training. It is therefore crucial that the administrators undergo some training in computer security.

4.2.4 Computer Physical Security

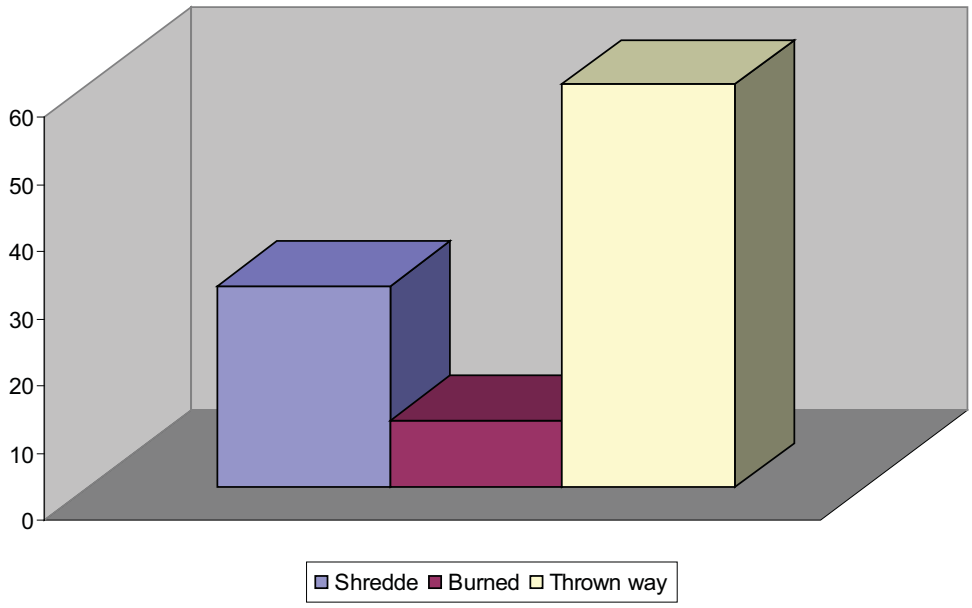
According to he system administrators, 100%, all computers are located in locked rooms and yet all of them could not agree on the number of computers at the College. It therefore means that computer security is considered in terms of safe rooms or locked rooms, and that even if an administrator has no knowledge of the number of computers available, the computer is likely to be safely locked. Access to the computer rooms, according to the system administrators, 80%, is only for authorized people. There is substantial number that still gets access to the computer rooms without authority, according to the system administrators,

20.0%.this percentage with access to computer rooms constitutes the threat to integrity of the computer security.

Keeping records on access to the computer rooms seems to be a popular practice in the physical security matters. This seems to be connected with room access conditions as those who keep records of access, 80.0%, equals those who say access is only for authorized persons. It can be concluded from the results that physical security seems to be taken more seriously than logical and administrative securities.

4.2.5 Security of access control Measures

Figure 4.5: Disposal of Computer Printouts



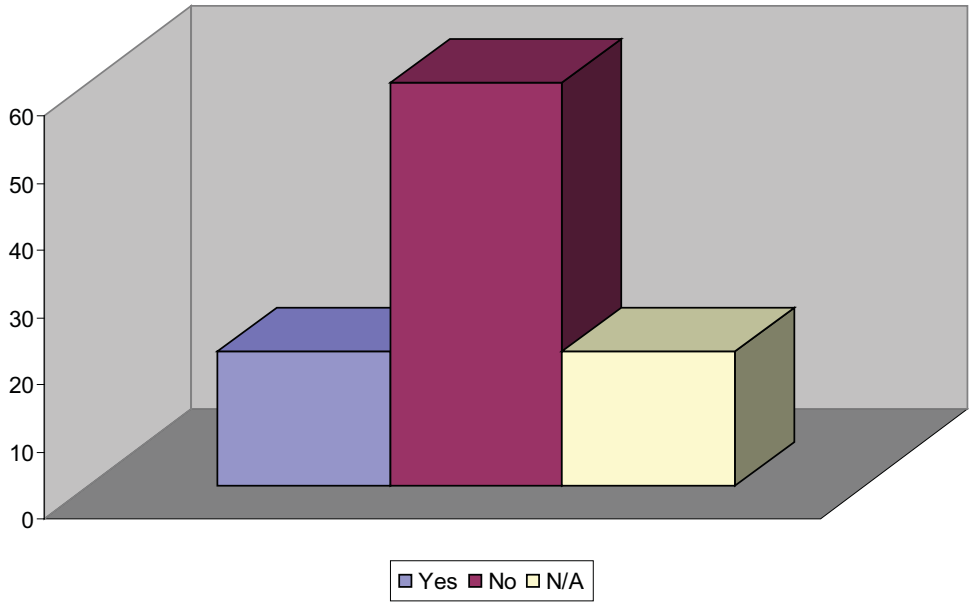
Print outs of the college computer laboratories or rooms are disposed of by throwing away. This can easily comprise passwords and software other access control measures. Printouts always constitute a security threat and a safe disposal method must be put in place. Seemingly, even the system administrators with training in computer security tend not to pay much attention to this security loophole. Printouts pose a threat in access controls security,

data file security and intrusion. Information on computer printouts can be used to compromise security of a computer system.

4.2.6 Use of back up.

There is nothing like complete security in terms of systems security. At one time, a computer is bound to fail and with it the information that has been created over time at a great cost. Regular back up of computer system is recommended and if disaster were to happen, one will have a fallback tool. It seems as if most system administrators do not pay attention to this important security matter. Of all the system administrators included in the survey, 60.0% indicted that back up is not done regularly. Every computer security system needs a regular backup as an essential practice. The college system needs to put this in place so that regular backups are carried out.

Figure 4.6: Backup Schedule



No remote backup system is available as 100% of those interviewed indicated lack of this facility. Remote backup is important when there is a failure especially for disaster recovery.

4.2.7 Use of Identification and Passwords as Access controls tools

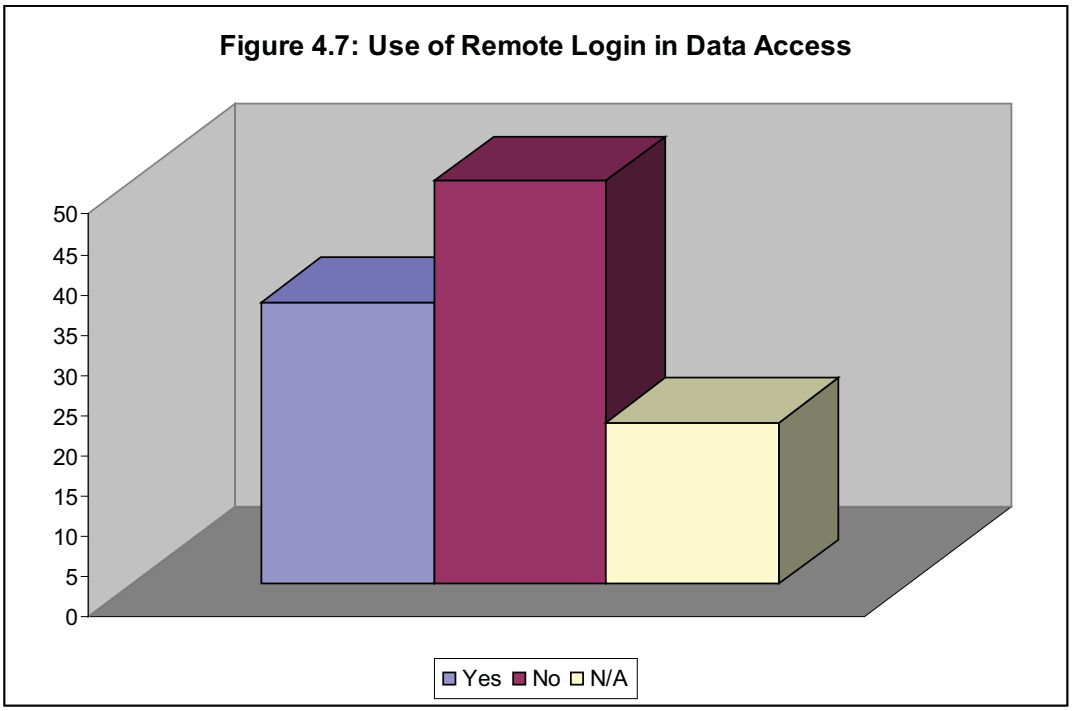
Identification and passwords are used to provide protection and security to the computer system and data files. Identification tool is mostly used to control physical access and should be reinforced with presence of security personnel who understand deception measures. Passwords are used to gain access to the computer system and if not used properly, can be a source of security risk and threat to the system. Use of password alone is not enough in system security especially in a network but the password should make it hard for hackers to gain access. It is therefore recommended that passwords be short, not easy to copy and not be within reach of prying eyes. According to most system administrators, 60.0%, some identification or password is required to gain access to computers at the college but 40.0% indicate that this is not necessary. It is this percentage where no identification is required that security risk and threat are defined in terms of system use. Administrators who allow use of computers without any form of identification or password constitute a risk to the security of computer systems at the college.

Table: 4.9: Use of Identity and Passwords in Computer Access

Q 14 Are users required providing user identification and passwords to gain access to computers?			
		Frequency	Percent
Valid	1 Yes	3	60.0
	2 No	1	20.0
Missing	System Missing	1	20.0
Total		5	100.0

Seemingly, default passwords are changed regularly according to most system administrators, 80.0%, and another 20.0% have indicated that passwords are not changed regularly. It seems that the system administrators do not understand well the use and risk of passwords.

4.2.8. Network Access and Control



Hackers to gain access to the communication ports of the system can use logging in from remote sites and this can then be used to gain access to the data file, to deny use of the system or to consume system resources. Although almost half of the administrators, 50.0%, do not log on from remote sites, and since backup is not in most cases done from the sites, some administrators, a sizeable number still use it. This introduces the concept of trust in access control, and trust can be a threat to the system.

Administrators in most cases, 80.0%, do not allow users to gain access to the command line and this seems to be considered a very good security measure. Since there are networks at the college, denial of access to the command line is no security because one can use the Trust terminal or gain access to the communication ports and still gain access to the command line. It should not be taken that denial to command line, though a good measure is ultimate security to data files and systems files.

In many administrative structures, it is basic practice that there is somebody responsible for maintaining user profiles for threats are most likely to come from those who understand the operations of the system. Users who no longer need the services of the system should be removed from the logging structure files. At the Loreto College, it seems that there are administrators responsible for keeping user profiles but the question is how this information is used in the security measures. Of the systems administrators interviewed, 60.0% indicated that user profile is maintained but 20.0% do not maintain user profiles. This 20.0% constitute a threat in terms of intrusion and data file security.

Control software is useful in access security measures, and the effectiveness of this tool is dependent on its currency, integrity and status of the system. Any system connected to the worldwide network or local area network cannot claim total security even if control software is available. Systems administrators mostly, 80.0% indicated presence of control software. This may be due to package terms when by new computers, training, and need to maintain system security.

Table 4.10: Access Control through Software

		Frequency	Percentage
Valid	1 Yes	4	80.0
	2 No	1	20.0
	3 N/A	0	0
Missing	System Missing	0	0
Total		5	100.0

Use of modems is essential in network operations but is also a security risk. Hackers can take control of modems and easily gain access to the communication port of the computers. Once this is done, passwords can be easily compromised especially in Microsoft operating systems. Many systems administrators give access to the systems through modem access and this constitutes a threat to the systems at the university. Password controls should therefore be strengthened and controlled properly.

Table 4.11: Modem Access

		Frequency	Percent
Valid	1 Yes	5	100
	2 No	0	0
	3 N/A	0	0
	Total	5	100

External access control mechanisms, in most cases, 100.0%, does not exist at the College in terms of network connection. This means access to files at the network system of the College is open to those who may want to gain unauthorized access.

Access levels control can be used as security measure in access control but because the College seemingly has no control system in the network, the access levels can not be used as complete security measure.

Users account control is another access control tool and this is seemingly non existent at the College as 100.0% of the systems administrators do not have it.

4.2.9 Terminal or Workstation Restrictions

Access to a terminal, physically or through a network, defines the threat to a system. If users are not restricted to defined terminals or workstations, it is very difficult to identify the source and type of security risk and vulnerability. According to most systems administrators, 80.0%, included in the sample, there is no restriction to terminal or logging on. If this is the case, then a user can easily gain access to other computers in the network posing a security threat to the information or data. Equally, unrestricted access to log on computation poses the threat of virus and espionage. Even if there are restrictions to terminals or workstations in terms of access, 20.0%, the majority of system administrators do not impose any restrictions. As long as those systems are on, part of the network access can be gained and hence pose a security risks.

Security risk is worsened by lack of restrictions on software use on terminals or workstations. Computer security risk threat levels vary with the type of operating system and application software in use. Some operating software and application software make it easy to access and gain control of other computers in the network. Systems administrators need to pay attention to this computer security risk and limit its threat.

4.2.10 Computer Security Guidelines and Documentation

Existence of computer security guidelines and documentation is considered a basic requirement in any computing environment. It encourages good practice in computer use as well as decrease bad intentions. Guidelines and documentation from the authority provide

strong measures against common security problems in the computing environment. In this study, systems administrators are considered as the implementers of College policy guidelines. Those guidelines should be in documented form. From the field survey, it is clear that no security system or directive on use and implementation of information systems is documented in approved form. All the systems administrators, 100%, in the survey acknowledged lack of such document.

Most servers and systems have documentation on configuration and this is usually provided for in the purchase of new systems or servers. The configuration document basically concerns hardware operations but not the administrative issues. Even if 80.0% of the interviewed systems administrators acknowledged the existence of system configuration document, it is neglected by lack of College Management Board guidelines and documentation.

4.2.11 Audit trails as security measures

Seemingly, no kind of audit exists in the computer environment at Loreto College. Audit trails are used to identify possible trouble spots in the software and hardware environments, what is available and what is lacking, and measures necessary. 40.0% of the systems administrators seemingly do not know what audit trails is and 60.0% do not practice it even if they know about it. This brings to question the level of training on computer security. Audit trails are one of the security measures recommended for any computer environment. The lack of audit trails is a reflection of the general lack of computer security policy at the College Management Board level.

Chapter 5 - Discussion and the Future

5.1 Introduction

As most organizations and people go online to carry out their transactions, or as people use the internet which is a kind of networking strategy, threats which are factors that pose as a danger to the network are likely to occur. It is the author's opinion that organizations should be very keen to introduce every kind of mechanism that would act as a means of security to their networks to avoid regrets to organizations. Based on the results of the data analysis this study makes the following conclusions and results.

5.2 Building a Secure Network

Security is a difficult topic and everyone has a varied concept of what security is and what levels of risks are acceptable (Michael, Hardie & Lamaster, 2001).

The key for building a secure network at the college is to define what security means to the college's authority. Once that has been defined everything that goes on with the network can be evaluated with respect to the policy.

It is important to build a system with security in mind and in such a way users are not always reminded of it.

It is important to get feedback of the users who find a security policy restrictive so this can be used to improve the policy.

Security is everybody's business and only with everyone's cooperation a security policy and consistent practices will be achievable.

After careful evaluation of research survey findings, the general observation is that Loreto computer network security should be addressed by rewriting its laboratory rules based on the check list that follow.

5.3 Secure Network Check List

The following must be considered in building a secure network;

5.3.1 Physical security

This is the most important part of maintaining the computer system and often overlooked by the administration because of their close proximity to the systems. Other factors include;

5.3.2 Network security

This is the second most important part in maintaining a system security. While good physical security can go a long way if you operate a network (e.g. internet connection) the system is vulnerable to outside attacks

5.3.3 Protocols/services

Computers will use different types of software and programs. It is likely that due to their heterogeneity people will have different understanding of security thus the programs will always have security holes that could be exploited.

5.3.4 User security

User security will vary depending on the nature of system that is running. If a user is running a server with very few users who will log into the system and use it directly then the security of a system will depend on the users' character.

5.3.5 Passwords

Passwords are widely used and they protect all user accounts, sensitive websites and system services. If one knows the right passwords, one can gain administrative privileges on a system where one may not even be a user or infiltrate an environment that has never even worked before.

5.3.6 System administration

Quality administration can make all the differences in security protection. Defense in depth is required in this protection where several layers of security are used. Many systems do self checks and changes. One needs to observe the usage patterns. Cracking tools can be run regularly. Put in place break-in deterrents. Security awareness to users is also another way of ensuring security. Keep users advised of the administrator's expectations of them in maintaining security. Currently at the college there is no mechanism for computer security planning or a forum to identify security issues and problems that should be resolved.

The study makes the following recommendations in security at the college:

5.4 Security planning and coordination

It is the recommendation of this study that the college constitutes a computer security committee reporting to the management board. The committee should comprise 11 student representatives, the administrative assistant, the laboratory assistant, the network administrator, and 4 course coordinators and chaired by the principal. Establishing such a committee would create a vehicle for ongoing planning and would help to ensure that the college's security efforts are coordinated and effective.

5.4.1 Responsibilities of the Committee

The information systems security committee will carry out the following duties;

- Ensure that information is created used and maintained in a secure environment.
- Ensure that all of the college's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all the computer users are aware of and fully comply with the policy statement and the relevant supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant Kenyan and international security legislation.

- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of information security.
- Ensure that all the computer users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle and that all the college owned assets have an identified owner /administrator

5.4.2 Committee Membership

For effective functioning, the computer security committee should have no more than 8 members as follows:

- 2 student representatives
- 2 coordinators
- 2 administrative representatives
- College legal officer
- Network administrator

The college management board should make changes in the committee membership as the need arises.

5.5 Computer Security Policy

Policies are necessary to ensure that important college teaching, research and administrative data, and other confidential information is protected from theft or unauthorized disclosure. Additionally state laws, for example the Data Protection Act, make the college legally responsible for ensuring that information is accurate and used appropriately.

In addition to fulfilling the legal obligations, complying with the information system security policy will ensure that the college offers a professional and effective service. If enforced the policy will make sure that computer users are aware of any legal requirements and the college policy that apply to them in their role in the college.

Breaking the rules will put us all at risk. By divulging sensitive information, or by not applying strict security controls to sensitive information in your care, you expose the information and the college to potential damage and loss.

5.6 Education and Training

All users of Loreto college computing and networking facilities are expected to read and abide by the respective regulations. The network administrator will be available to provide advice and training in all areas of information security. The researcher is part of the staff that oversees security as well in the college and will assist in the said training. Staff, students and any third parties authorized to access the college network should use the systems and facilities as stated by the security policy in Appendix A of the thesis report.

5.7 Incident Detection and Response

In the event of a security breach, we will contact our network administrator. The office is expected to have a one-hour response policy during office hours and a twenty four hour response policy at all other times to deal with serious incidents, such as virus infections. In addition, the network administrator will monitor the server and firewall regularly to make sure that no breaches have occurred.

5.8 Future Research

In this paper, a number of threats that are common to computer systems and that deserve careful concern to the students, staff and managers have been discussed. The common controls that are the countermeasures to the threats have also been explained. They are physical, electronic, software and management controls. It has been explained that, as systems change, there will always be new threats to computer systems. Thus, there is need to devise new ways to counter these threats. It is also important to mention that, it is has been

hard to exhaustively cover all the threats and counter measures that exist in a paper of this size. This is partly because every organization exists in a different environment from the other and has a different mission and vision. This then serves just a summary of what would have been a large report.

There is need to conduct further survey in computer security at other Loreto branches in terms of security practices and policy implementation. The need to share resources among academic institutions requires increased network security measures in terms of a common security policy. There is also need to make technical analysis and develop more comprehensive models to manage and monitor computer network components.

References

Whitman, M. E. & Mattord, H. J., (2005) Principles of Information Security Second Edition

Whitman, M. E. & Mattord, H. J., (2005) Principles of Information Security Second Edition

Whitman, M. E. & Mattord, H. J., (2004) Improving Information Security through Policy Implementation In: *Proceedings of the 7th Annual Conference of the southern Association for Information Systems*

Mark Ciampa (2005) security+ Guide to NETWORK SECURITY Second Edition

Randy Weaver (2007) A Guide to NETWORK DEFENSE AND COUNTERMEASURES Second Edition

Pfleeger, C., P. & Pfleeger S.L., (2006) Security in Computing Fourth Edition. Prentice Hall

Loudon, C. K. & Loudon, J.P., (2006) Management Information Systems Managing the Digital Firm Ninth Edition Prentice Hall of India

Bishop, M. (2006) Computer Security: Art and Science Boston: Addison Wesley

Schneider, B. (2000). Secrets and Lies: Digital security in a networked world. John Wiley and sons Inc

Stefanek, G. L (2002) Information Security Best Practices, 205 Basic Rules Elsevier, USA

Von Solms, H. S. & Eloff, J. H. (2001) Information Security First edition Amabhuku publications (Pty) Ltd 2000/1/2, RAU, Republic Of South Africa.

Ralph Stair, George Reynolds (2008). "Principles of information systems" A Managerial approach, Eighth Edition

Robert Schultheis & Mary Sumner (1995) "Management Information Systems" The Manager's View, Third Edition

Freer, J, (1990): Computer Communications and Network

Que. Corporation, (1994): Introduction to Networking

Digital Equipment Corporation, (1996): Digital UNIX

Symantec Corporation, (2008): Norton Internet Security

Hoffman, L.J, (1977): Modern Methods for Computer Security and Privacy

Sheldon, T, (1996): Windows NT security Hard-book

Reinhardt, R.B, (1993): An architectural Overview of Unix network Security

Frost, J, (2000): Windows 2000 Security

R.T. Morris, (1985): *A Weakness in the 4.2BSD UNIX TCP/IP Software.* Computing Science Technical Report No. 117, AT & T Bell Laboratories, Murray Hill, New Jersey

Bellovin, S.M, (1989): *Security Problems in the TCP/IP Protocol Suite.* Computer Communication Review, Vol. 19, No. 2, pp. 32-48

Rekhter, Y; Moskowitz, R; Karrenberg, D; de Groot, G; and Lear, E: "Address Allocation for Private Internets." RFC 1918

J.P. Holbrook; J.K. Reynolds: "Site Security Handbook".

Sobol, M; C. Hardie & E. Lamaster, (2002): The Security Audit: An Introduction and Practical Guide. PESTPATROL, protecting computers from hidden threats Technical white paper

The New Lexicon Webster's Encyclopedic Dictionary of the English Language

New York: Lexicon

APPENDIX A

REWRITTEN SECURITY POLICY

CONDITIONS FOR USE OF COLLEGE COMPUTING FACILITIES

1.0 OVERVIEW AND CONDITIONS

Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.

2.0 SCOPE AND PURPOSE

The purpose of this document is to provide the Loreto College fraternity with an information system security policy. The document has been developed to guide computer users and anyone else on security matters. The policy applies to all staff, contractors, consultants, temporary workers and part time lecturers, and other workers at the college. The policy applies to any and all persons who have any form of computer account requiring a password on the Loreto college network including but not limited to a domain account and e-mail account. The policy also applies to all equipment that is owned or leased by the college.

It shall be the responsibility of the computer department to provide adequate protection and confidentiality of all corporate data and proprietary software systems whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized computer users at the college, and to ensure that data configuration controls are in place. Please note that non-compliance may lead to disciplinary action being taken.

3.0 THE TERMS USED

The following are some of the terms used in the information system security document;

"Account" means a user name or other identifier, which, with or without a password, allows a user to access computer system facilities.

"Computer users" means a group of persons belonging to a particular class, e.g. college students or teaching staff.

"Authorized user" means having been given approval to use an account by the network administrator of the computing services or his/her nominee or a teaching member of staff.

"Computing Resource" means any measurable quantity supplied by the facilities including, but not restricted to, central processor time, disk space, disk block transfers, memory, connect time and stationery.

"Relevant resource" means a person appointed by the college on behalf of the network administrator whose role is to control use of computing resources allocated to his/her class or section.

"Facilities" means the computing infrastructure such as the processing equipment.

"Third party" means a person or organization normally external to the college who has entered into a contract with the college to use the facilities.

"College" means the Loreto College.

Note that the network administrator may suspend the user's right of access to the facilities for a period not exceeding four weeks and may additionally refer any matter to the principal of the college to be dealt with under as stated below;

The Principal may suspend the user's right of access to the facilities for such period as the Principal considers suitable and action may also be taken. The Management Board of the college may further the withholding of the facilities from any person for any period without stating a reason.

Since improper use of the information system assets can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to the policies below may be subject to disciplinary action up to and including dismissal from the college.

All computer users that have access to organizational computer systems must adhere to the approved application policy in order to protect the security of the network, protect data integrity, and protect computer systems.

4.0 Security Policy and Procedures

4.1 General Use and Ownership

- Users should be aware that the data they create on the corporate systems remains that property of the college. The management cannot guarantee the confidentiality of the information stored on any college network device belonging to it.
- Employees are responsible for exercising due care regarding the use of college's information resources. Guidelines concerning personal use of systems are clearly defined in the security policies that follow. In the absence of any such policies, employees should be guided by their departmental policies or should consult their supervisor or line manager.
- For security and network maintenance purposes, authorized persons within the college may monitor equipment, systems and network traffic at any time without the staff and students' consent.
- The college reserves the right to audit network and systems on a periodic basis to ensure compliance with the policy.

4.2 Security and Proprietary Information

- Examples of confidential information include but are not limited to the college corporate strategies, competitor sensitive information, trade secrets, specifications, customer lists and research data. Staff and students should take all necessary steps to prevent authorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User –level passwords should be changed every 30 days.
- All computers and laptops should be secured with a password-protected screen-saver with the automatic activation feature set at 10 minutes or less or by logging off when the system will be left unattended.
- Encrypt information when necessary.
- Posting by computer users from the college e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the college.
- All computers used by a computer user that are connected to the college's network, whether owned by the user or the college, must be continually executing approved virus-scanning software with a current virus signature.
- Staff and students should exercise caution when opening e-mail attachments received from unknown senders.

4.3 Unacceptable Use of Facilities (Enforcement)

Computer users' activities that shall violate the security policy are prohibited and under no circumstances will an authorized computer user of the college shall engage in any activity that is illegal under local state or international law while using the college owned resources. The lists that follow are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use. Non-compliance shall lead to disciplinary action being taken i.e. any computer user found to have violated this policy may be subject to

disciplinary action, up to and including demotion or termination of employment for the staff and expulsion or other penalties for the students.

4.4 System and Network activities

4.4.1 User Identification and Passwords

- Each user shall be allocated an individual user name and password. Account passwords must not be written down, disclosed or allowed use by others. The owner of a particular user name will be held responsible for all actions performed using this account.

- Requests for new computer accounts and for termination of existing computer accounts must be formally authorized to the network administrator or the relevant manager. Requests for additional access to specific business applications must be authorized in writing to the network administrator or the relevant manager or by the relevant application owner.

- Staff must notify the network administrator or the relevant manager when moving to a new position or location within the college. This ensures that the necessary setups to provide fast access to the most appropriate mail and file servers can be put in place. Staff and students are not permitted to take computer equipment when moving to another position within the college.

- Line management must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential client information and moves to another role where this access is not required. It is a security breach to access an account or information of which the staff is not intended to access.

- All user accounts must have the following password settings: Minimum password length of 8 characters, a combination of alpha, numeric and punctuation should be used. Users are forced to change their passwords by the system every 30 days. Users will not be able to repeat passwords.
- Accounts are locked after 3 incorrect login attempts.
- Passwords must not be easily guessed (i.e. names, months of the year, days of the week, usernames, etc. must not be used as passwords). If guessed the cracker will be responsible for the measures enforced. This requirement if not adhered to; the user will be alerted on the screen.
- All users must not circumvent user authentication or security of any host, network or account.
- The computer system will automatically disable accounts that remain inactive for 60 days.

4.4.2 Access to Information

- All information held on the networks including email, file systems and databases are the property of the College and staff should have no expectation of privacy for this data.

- Using the college computing resource to actively engage in transmitting e-mail messages or any other form of material that is in violation of sexual or any other form of harassment or hostile workplace laws in the user's local jurisdiction is prohibited.

- Although it is not a general practice of Loreto college to monitor stored files, email messages and internet access for their general content, the college reserves the right to do so for the protection of computer users, for system performance, maintenance,

auditing, security or investigative functions (including evidence of unlawful activity or breaches to Loreto policy) and to protect itself from potential corporate liability.

- Requests to access the computer account of a member of staff or student who is absent from the office or the laboratory must be directed to the network administrator in writing by the relevant manager. The access is given effect by changing the user's password and allowing the relevant manager or a colleague to access the account directly. Where this access is granted it must be used for enquiry purposes only.

- Staff and students must not issue any college information to third parties unless they have authorization to do so.

- Users are only permitted to access electronic information and data that they require to perform their duties.

- If confidential information is lost, either through loss of a notebook computer, backup media or other security breach, the network administrator or the relevant computer department resource person must be notified immediately.

- All computers must be switched off at the end of the day. This action erases residual information contained in the computer's memory and assists with overnight anti-virus software updates.

4.4.3 Data Protection Act

- The Data Protection Act (1999) imposes responsibilities on users regarding the processing of personal data. Personal data refers to data relating to a living individual who can be identified either from the data, or from the data in conjunction with other

information held by an organization. It is the responsibility of all Loreto college staff to ensure that the principles of the Act are complied with.

- All computer users must read the Data Protection Act which is in the Loreto College Library.
- Violations of the rights of any person or college protected by copyright, trade secret or any other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of software products that are not appropriately licensed for use at college is strictly prohibited.

4.4.4 Personal use of computer systems

- While Loreto college personal computers are provided for the business use such as teaching and research it is not acceptable to use them for personal use.
- Staff must not use the college computer systems or the internet for commercial activities that are not related to the business of the college.

4. 5 Personal computer Security

- Computers must not be left unattended for long periods while signed-on e.g. during lunch, coffee breaks etc. Users must either logoff or activate a password-controlled screensaver if they are leaving their personal computer. The screensaver should be set to activate by default after 10 minutes of inactivity.
- Information technology equipment must not be removed from the college premises unless a written approval has been received from the network administrator or the relevant manager. An exception is made for authorized off-site back-ups provided

they are adequately protected against unauthorized access and this must be signed for before being removed from the college premises.

4.5.1 Software

- Software must not be copied, removed or transferred to any third party or non-organizational equipment such as home PCs without written authorization from the computer department.

- Only software that has been authorized by the network administrator may be used on the college's computers connected to the college network.

- Downloading of any executable files or software from the internet is forbidden without written authorization from the network administrator or the relevant manager. Staff and students may be given this authorization based on their specific work requirements.

- Regular reviews of desktop software are undertaken and the presence of unauthorized software will be investigated. The college reserves the right to remove any files or data from the computer systems including any information it views as offensive or illegal without any consultation from the computers users.
- All alterations to system and application software must follow strict change control procedures to ensure the integrity of the college computer systems. For major changes this should include: authorization of request for change; risk assessment of change; user acceptance testing; relevant management sign-off; computer security sign-off; roll-back procedures in the event that the change failed; and documentation of the above.

- Software development and testing must be carried out on a separate server from the live environment.

- Adequate controls should be in place over any test data that is used in the testing process, as this data quite often is a mirror of live data.

4.5.2 Confidentiality

- Confidential data held on computer media (e.g. Disks) must be stored securely when not in use.

- Any computers for disposal must have the hard disk wiped clean before they are distributed outside the college.

4.5.3 Portable Computers

- All reasonable precautions must be taken to protect equipment against damage, loss and theft. The equipment must not be left unattended in any public place. Damage, loss or theft must be immediately reported to the information technology relevant manager

- Data must be backed-up to the network on a regular basis and notebook users must ensure that the data on their notebook computers is adequately backed up.

- Portable computers must be set with a switch on pin number and must not be used to store sensitive information.

- All portables must be locked to a physically secure object when in use using the key and lock provided. Portables must be stored securely when not in use. Staff and students must not leave a portable computer unattended at any time when not secured.

4.5.4 Computer Viruses

- Corruption of personal computers or portable's data or software by malicious software (e.g. a computer virus or a worm) must be reported to the network administrator.
- Introduction of a script or malicious programs into the college network or servers such as viruses, worms and Trojan horses is prohibited.
- Port scanning and packet sniffing or any other form of security scanning by users is expressly prohibited.
- Users are not permitted to disable or remove antivirus software under any circumstances.
- Unauthorized screen savers are not permitted, as they are a potential source of computer virus. Computer users must contact the network administrator for advice.
- Virus checking must be performed by the network administrator or the relevant manager on all software prior to installation or distribution within the college.
- Virus checking software must be installed on all the college computers and must be automatically executed at system start-up.
- All computers and servers must be updated with virus signature files any time at system start up.

4.6 Internet and Email Security

4.6.1 *Internet*

- All computer users have a responsibility to use the internet in a professional, ethical and lawful manner. Users must regard internet access as a privilege, which can be revoked at any time.

- Computer users should exercise caution when making payments over the internet, as the security of credit card details cannot be guaranteed. The College will accept no liability for losses arising through the transmission of personal or financial information over the Internet.

- Users must not use Loreto College internet facilities to download, display, generate and/or pass on to others material whether in text, pictures or any other form, which would be regarded as offensive. It is important to note that what constitutes offensive material is not one for the sender to determine. It is the effect on anyone viewing the material that is considered important. In law, possession of some material is deemed to be a serious criminal offence, whether in the workplace or otherwise.

- All access to the internet from Loreto College network will be via an approved channel that will be secured by a firewall. This shall be set up by the network administrator.

- Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the internet, failing to exit from websites, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the internet. Note that the computer system stores an audit trail on the user's usage of the computers.

- Users must not use the same passwords for login to Internet websites as they do internally for Loreto College computer systems.

- Loreto College reserves the right to review, audit, intercept, access and also discloses all access to the internet. This includes emails sent and received in addition to websites visited and files downloaded from the internet.

4.6.2 Email

- Email users must exercise caution with any external attachments other than those received from a trusted source, as these attachments may contain a computer virus. All emails will be scanned automatically by the computer system and any existence of a malicious code will be displayed on the computer screen.

- Users must not represent themselves as another individual in electronic communications.

- Email users must be aware of the risks associated using email to send confidential or commercially sensitive information. The unauthorized use or forging of e-mail header information is forbidden.

- Users must ensure that documents attached to emails are not copyright protected.

- As email is a form of publishing and covered by relevant publishing Acts, libelous and defamatory material is not permitted.

- Users should be aware of their obligations under the Data Protection Act and must not use email for transmitting data of a personal nature related to a third party.

- If any person receives email, which they deem to be inappropriate, offensive or illegal, they must inform their relevant manager. Immediate reporting of incidents facilitates more successful identification of the source and other details.

- All emails that are sent externally must carry a standard Loreto College disclaimer. Users must not attach their own disclaimers to emails.
- Computer users must not be involved in the solicitation of –email for any other e-mail address, other than that of poster's account with intent to harass or collect replies.
- Software is in place to monitor incoming and outgoing external email messages. Messages that contain text which indicate that they may have come from an unsolicited source are quarantined by the software and an automatic email is sent to the Loreto College sender or recipient to inform them that a message has been stopped. Please contact the network administrator relevant manager if you receive a quarantine message.

4.7 Remote Access

- Remote Access can be defined as access to Loreto College. It is any computer system resources or data from a location external to the college. This access may be by a third party or a college authorized computer user who is located off-site.

- All portable computer users must ensure that they have remote access software to connect securely to the Loreto College computer systems.

- For cost and other security reasons remote connections must be closed as soon as a search is completed.

- Telephone numbers that are used to access the college computer network must not be listed in public telephone directories and must not be disclosed to unauthorized persons.
- All inbound and outbound communications to the college private network must be routed through the proxy sever.
- Where dial-up communications are used, the college name or logo must not be revealed until all security validations have been successfully established.

4.8 Third Party Access

- Third Party Access can be defined as the granting of access to Loreto College computer network. The computer resources or data to an individual who is not a student or staff of the college. Software vendors who are providing technical support, Contractor or consultant, Service provider; and an individual providing outsourced services to the college requiring access to applications or data are examples.
- Third Party Access can only be provided after the Third Party has signed a confidentiality agreement that must be included in their formal contract with the college. Staff and students must never permit another individual to utilize their user name to access the college network.
- Further requirements for granting Third Party Access are: Risk analysis process, approval by data owner, approval by the network administrator or the relevant manager.
- Third party access will only be permitted to facilities and data which are required to perform specific agreed tasks as identified by the college.

4.9 Software Licenses

Copyright stipulations governing vendor-supplied software must be observed at all times.

- The network administrator or the relevant manager is responsible for maintaining records of software licenses. Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions.

- All software developed within Loreto College is the property of the college and must not be copied or distributed without prior written authorization from the network administrator.

4.10 Data Backups

- The network administrator or the relevant manager must take daily backup of the main servers for which they are responsible for managing. This may be automated by the network administrator to take effect in a suitable time of the day.

- Computer users must always save data and files on the network as opposed to the local hard disk. This ensures that the regular backups are taken and are available for recovery purposes. Users should be aware that data saved on their local hard disk is not backed up by the network administrator or the relevant manager.

- Where emergency changes are made to production files or software, these changes must be authorized by line management. The resulting audit trail must be retained.

- All application systems that handle sensitive Loreto College information must generate logs that show additions, modifications, and deletions to such sensitive information.

- Operating systems handling sensitive, valuable, or critical information must securely log all significant computer security relevant events.

- Security reports and audit trails must be reviewed on a monthly basis and all violations accounted for.

- All login screens must include a warning against unauthorized use of the college computer systems and a notification of the college right to monitor user activity.

- The use of privileged accounts such as the network administrator must be restricted to authorized persons only. The passwords must be held securely and their use will be recorded and checked on a regular basis.

- When computer users have logged in, they should be restricted to menus that show the options that they have been authorized to select by the network administrator. All end-users must not be allowed to invoke operating system level commands.

4.11 Physical Security

The following standards must be applied to computer room access at all times:

- Access to the computer operations rooms must be restricted to authorized personnel only.

- Third parties who have been granted access to the computer operations rooms must be accompanied at all times by authorized persons.

- Access to the computer operations rooms must be controlled by a physical access control mechanism such as an electronic or combination lock.

- The computer rooms must be fitted with smoke/fire detectors and fire extinguishing equipment, which should be set to automatic operation when the computer room is left unattended for long periods.
- Fire detection and prevention equipment must be tested at least twice a year.
- Incase of fire all people should assemble at fire assembly point.
- Each production server must have a UPS installed to protect against power surges and the UPS and generator must be tested every 3 months.
- Computer media e.g. tapes and documentation must be stored securely, e.g. in locked cabinets, when not in use.
- Magnetic media that is no longer required and which may contain confidential data must be disposed of securely, i.e. all data must be erased or the media must be rendered inoperable.
- Back-ups of sensitive, critical, and valuable information must be stored in an access-controlled site.

APPENDIX B

COMPUTER USER AGREEMENT

I acknowledge that I have received, read and understood the above Information Resources Acceptable Use Policy. I understand that I must comply with the information security policy when accessing and using the information system assets and my failure to comply with the policy shall result in an appropriate disciplinary action and / or action by law enforcement authorities in the College or the Government.

Signature_____Date_____

PrintName_____

APPENDIX C

Computer Users' Questionnaire

The purpose of this questionnaire is to collect any information regarding the security of our computers and data for the purpose of analysis.

Any information provided will be treated with most confidence and the source will not be disclosed For each question, at least three responses are provided.

Please tick the appropriate response and return the questionnaire to Paul M. Mwai of Loreto College.

1 Do you require a password to use a computer?

YES	NO	N/A

2 Do you think it is important to use a password to access a computer?

YES	NO	N/A

3 The computers you use where are they located?

YES	NO	N/A

4 If the computer is in your office, do other people use it?

YES	NO	N/A

5 If you share computers with others, is there a register or booking form where users notes their names and time period when computers are used?

YES	NO	N/A

6	Do you think that it is important to maintain a computer usage receipt?	YES	NO	N/A
7	Do you think that your computer is secure in the current location?	YES	NO	N/A
8	Do you change your password periodically?	YES	NO	N/A
9	Do you think it is important to change the password periodically?	YES	NO	N/A
10	Do you log off your workstation when not in use?	YES	NO	N/A
11	Is there harm when you leave your work on the screen?	YES	NO	N/A
12	Is your password noted on or near your workstation?	YES	NO	N/A
13	Is there risk in sharing your password?	YES	NO	N/A
14	Do you think it is important to have lengthy passwords that combine letters and numbers?	YES	NO	N/A

15	Does your computer go off immediately when power goes off?	YES	NO	N/A

16	Do you have somebody whom you contact when your computer develops problems?	YES	NO	N/A

17	Do you make copies of your work?	YES	NO	N/A

18	If you do, how often?	YES	NO	N/A

19	Do you think it's important to make copies of your work?	YES	NO	N/A

20	Do you use diskettes?	YES	NO	N/A

21	Do you store your disks away from your computer?	YES	NO	N/A

22	Do you think it is important to keep diskettes away from your computer?	YES	NO	N/A

23	Is there a procedure for disposals of print outs?	YES	NO	N/A

24	Is there harm if you just throw them away?	YES	NO	N/A

25	Do you share computer files with others?	YES	NO	N/A

26	Are there other people able to access your work on your computer?	YES	NO	N/A

27	Is there any harm in other people accessing your work?	YES	NO	N/A

28	Do you know that people can destroy your work?	YES	NO	N/A

29	Do you know that people can disclose the contents of your work?	YES	NO	N/A

30	Do you know that disaster can happen and you could lose your computer equipment?	YES	NO	N/A

31	Do you find it risky to store data in a central computer	YES	NO	N/A

server?

32 Does the computer you use have anti virus?

YES	NO	N/A

33 Are antivirus of any use when loaded in your computer?

YES	NO	N/A

34 Have you ever had your work destroyed by a virus attack?

YES	NO	N/A

35 Have you ever lost work on your computer or disk?

YES	NO	N/A

36 Are your computers connected to the college network?

YES	NO	N/A

37 Are the computers serviced regularly?

YES	NO	N/A

38 Do you access the internet?

YES	NO	N/A

39 Do you use the college network to access the internet?

YES	NO	N/A

40 Do you download anything from the internet?

YES	NO	N/A

41 Do you think there is any harm in downloading things from the internet?

YES	NO	N/A

42 What programs do you use?

a) operating systems:

Windows-XP	
Windows2000	
UNIX	
Netware	
Linux	

b) word processors:

Ms word	
Word-perfect	
Others	

c) spread sheets:

Ms excel	
Lotus123	
Super-Calc	
Others	

d) database programs:

Ms access	
Dbase-III plus	
SQL server	
Oracle	
Others	

e) Others:

Accounting	
Statistical	
Programming	
Others	

APPENDIX D

System Administrators' Questionnaire

The purpose of this questionnaire is to collect any information regarding the security of our computers and data for the purpose of analysis. Any information provided will be treated with most confidence and the source will not be disclosed. For each question, at least three responses are provided. Please tick the appropriate response and return the questionnaire to Paul M. Mwai of Loreto college.

1	Any formal training on computer security issues?	YES	NO	N/A

2	Do you or any other person train users on security issues?	YES	NO	N/A

3	Do you have any documentation on computer security issues for users apart from the lab rules?	YES	NO	N/A

4	Do you think documentation and training would play a major role in preserving security of our computer -resources?	YES	NO	N/A

5 To the best of your knowledge, how many;

a) Computers do we have at college?

b) users of email Do we have at college?

c) computer servers do we have at college?

6 Are computers located in locked computer rooms?

YES	NO	N/A

7 Who has access to the rooms?

a) authorized people

b) everybody

c) anybody

8 Is access to rooms recorded?

YES	NO	N/A

9 How are computer printouts disposed?

a) shredded

b) burned

c) thrown away

10 Are back up done regularly?

YES	NO	N/A

11 Do you have a remote backup system?

YES	NO	N/A

12 Are back up stored away from the site?

YES	NO	N/A

13	Does recovery procedures documentation exist?	YES	NO	N/A
14	Are users required to provide user documentation and passwords to gain access to computers?	YES	NO	N/A
15	Are default passwords changed?	YES	NO	N/A
16	As a system administrator, do you login from a remote site e.g. from home?	YES	NO	N/A
17	Do you have access to command lines e.g. (CMD)?	YES	NO	N/A
18	Can any other person maintain user profiles on your behalf?	YES	NO	N/A
19	Is there access control software to control user access to resources?	YES	NO	N/A
20	Is there MODEM access (dial up)?	YES	NO	N/A
21	Are there mechanisms for controlling access from	YES	NO	N/A

outside the network?

22	Are there documentations and approved procedures for adding a new user, modifying user access privileges And terminating a user from the system?	YES	NO	N/A

23	Do you have procedures for determining access levels?	YES	NO	N/A

24	Are users grouped and allocated accounts in a privileged manner?	YES	NO	N/A

25	Are there restrictions to what software terminal or workstation can run?	YES	NO	N/A

26	Are there restrictions to what specific terminal or workstation that a user can use to log on?	YES	NO	N/A

27	Are there security statements or directives on use and implementation of information systems written and Approved by the college management's board?	YES	NO	N/A

28	Are there servers and systems configuration documented?	YES	NO	N/A