VOT 71510

RISK ANALYSIS OF CYBER-CAMPUS MODULES (SECURITY GUIDELINES OF ELECTRONIC ACADEMIC ASSETS)

(ANALISA RISIKO MODUL KAMPUS SIBER - PANDUAN KESELAMATAN ASET AKADEMIK ELEKTRONIK)

SUBARIAH IBRAHIM
MAZLEENA SALLEH
NORAFIDA ITHNIN
RABIAH AHMAD

Department of Computer System & Communication
Faculty of Computer Science and Information system
UNIVERSITI TEKNOLOGI MALAYSIA

2003

VOT 71510

RISK ANALYSIS OF CYBER-CAMPUS MODULES (SECURITY GUIDELINES OF ELECTRONIC ACADEMIC ASSETS)

(ANALISA RISIKO MODUL KAMPUS SIBER - PANDUAN KESELAMATAN ASET AKADEMIK ELEKTRONIK)

SUBARIAH IBRAHIM
MAZLEENA SALLEH
NORAFIDA ITHNIN
RABIAH AHMAD

RESEARCH VOTE NO.
71510

Department of Computer System & Communication
Faculty of Computer Science and Information system
UNIVERSITI TEKNOLOGI MALAYSIA

2003

ACKNOWLEDGEMENT

Alhamdullilah, the research project for risk analysis of electronic academic assets is finally completed. With that, I would like to say thank you to those who has contributed to the success of this project directly or indirectly.

Firstly, I would like to express my gratitude to RMC for its financial support which has made it possible for the completion of this project. Special thanks to RMC staff, Puan Zarina, for her help in various clerical work regarding the project. Thank you too, to FSKSM staffs who has somehow contributed indirectly to the success of this project especially to those who participated in answering the questionnaires for this project.

Not forgetting my co-researchers, Puan Mazleena Salleh and Cik Rabiah Ahmad and Puan Norafida Ithnin, special thanks to all of you for your corporation in the success of this project.

I also would like to thank my research assistants, Shah Rizan Abdul Aziz, who assisted in the running of this project and Norsidah Taib who assisted in preparing this report.

Last but not least, I wish to thank my husband, Assoc. Prof. Dr Mohd Salihin Ngadiman for his support in my research participation.

Puan Subariah Ibrahim,

Project Leader.

ABSTRACT

RISK ANALYSIS OF ELECTRONIC ACADEMIC ASSETS

(*Keyword: Risk Analysis, Computer Security, Security Guideline*)

As the country moves into the Information Age, the use of Information and Communication Technology (ICT) has become a ubiquitous activity in the university departments for academic and administrative purposes. University academic information resources are valuable assets and the security of these assets should be managed properly. Without proper security measures and controls may result in the compromise, improper modification, or destruction of the information resources. This project focuses in outlining the security guideline that can be followed by academic staffs and others who are responsible for the security of electronic information in a university environment. The guideline addresses issues such as choosing good passwords, preventing virus attacks, e-mail security, pc intrusion and administrative responsibilities for the users and administrators who manage computers and networks. Risk analysis technique is used as a guidance in order to come out with the security guideline that is suitable for FSKSM. The guideline is simple and short enough so that it is easy to understand and followed by all levels of staffs. The security guideline formulated can be used as a starting point in drafting a security policy at UTM. With the application of security policy in the academic environment, the security of academic assets can be enhanced and the network as a whole can be trusted.

Key Researchers:

Puan Subariah Ibrahim (Head)

Assoc. Prof. Mazleena Salleh

Puan Norafida Ithini

Cik Rabiah Ahmad

E-mail: subariah@fsksm.utm.my

Tel. No.: 07-5576160-32386

Vote No.: 71510

ABSTRAK

PANDUAN KESELAMATAN ASET AKADEMIK ELEKTRONIK

(*Katakunci: Analisis Risiko, Keselamatan Komputer, Panduan Keselamatan*)

Apabila negara menuju ke era maklumat, penggunaan Teknologi Maklumat dan Komunikasi (ICT) menjadi aktiviti yang tidak asing lagi di kalangan warga universiti sama ada bagi tujuan akademik mahu pun pentadbiran. Sumber-sumber maklumat akademik sesuatu universiti adalah asset yang amat berharga dan keselamatan asset ini perlulah diurus dengan baik. Tanpa tindakan dan langkah-langkah keselamatan yang betul boleh mengakibatkan kecurigaan Maklumat akibat daripada kemungkina sumber-sumber Maklumat di ubah atau dirosakkan. Projek ini menyediakan garis panduan yang boleh diikuti oleh staf akademik mahupun staf lain yang bertanggungjawab terhadap keselamatan Maklumat elektronik dalam persekitaran universiti. Garis panduan ini memberi perhatian terhadap isu-isu seperti memilih kata laluan yang baik, menghalang gangguan virus, keselamatan e-mel dan pencerobohan PC. Selain daripada itu projek ini jug menggariskan tanggungjawab-tanggungjawab pentadbiran bagi pengguna dan pentadbir rangkaian yang mengurus komputer dan rangkaian. Teknik analisa risiko digunakan sebagai panduan bagi menghasilakn garis panduan yang sesuai untuk FSKSM. Garis panduan ini ditulis dengan mudah dan ringkas supaya ia mudah difahami dan diikuti oleh semua peringkat staf. Garis panduan keselamatan ini boleh digunakan sebagai permulaan bagi menyediakan polisi keselmatan ICT di UTM. Dengan penggunaan polisi keselamtan dalam persekitran akademik, keselamatan asset akademik boleh ditingkatkan dan rangkaian di universiti juga memperolehi kepercayaan awam.

Penyelidik Utama:

Puan Subariah Ibrahim (Head)

Assoc. Prof. Mazleena Salleh

Puan Norafida Ithini

Cik Rabiah Ahmad

E-mail: subariah@fsksm.utm.my

Tel. No.: 07-5576160-32386

Vote No.: 71510

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Introduction

In accordance with University Teknologi Malaysia's (UTM) mission to become a world-class university, it is expected that more Information and Communication Technology (ICT) will be employed in the daily operations of UTM. For example e-learning project is on its way whereby lecture notes are to be put up in cyberspace so that students can have access to it. Besides this, there are many more applications that utilized ICT that are being used in UTM such as students' registration, students' records and staff payrolls. Academic staffs use personal computers (PC) for both research and teaching activities. They prepare their lecture notes using PC and keep examination questions and students results in the hard disk of their PCs. Research findings and publications are also kept in the hard disks. Communications amongst staffs are also done through e-mail. Some staffs attach confidential data such as examination questions and results along with e-mail messages to their colleagues.

However, the benefits of ICT come with commensurate risks. Applications that employ ICT are more vulnerable to threats such as virus attacks, intrusions and denial of service. Confidential information can be intercepted while traversing through the network. In 2001 alone, some 52,000 attacks on computer network were reported to a Carnegie Mellon University center that coordinates computer emergency responses (H.E., Cox Newspaper, 2002). UTM web sites were also attacked several times. Some students impersonate as lecturers through e-mail messages during exam weeks in order to get examination questions. Hence the awareness of threats and vulnerabilities amongst staffs is needed and a proper security management is vital in order to reduce these attacks. If an organization often received attacks, the public's confidentiality towards the organizations might be reduced.

In order to reduce risk and encounter the loss of confidentiality, integrity and availability, an effective management of information security must be integrated within an organization's overall management plan.

Initially, this project is meant to be based upon Risk Analysis of Cyber Campus Module. However due to the unavailability of the module, we convert our research to security guidelines of electronic academic asset. Since academic assets are important and require various security services, namely confidentiality, integrity and availability, this project focuses in outlining the security guideline that can be used by members of faculty in order to address the above security concerns.

In order to come out with the security guideline which is suitable for FSKSM, an analysis of what assets to protect and what to protect it from is carried out by using risk analysis technique as a guidance. To achieve the goal of this project, the guideline must be simple and short enough to ensure it is easy to read, understood and follow. The guideline addresses issues such as choosing good password, preventing virus attacks and PC intrusion. It defines the security responsibilities of both the users and the people who maintain computers and networks in the faculty.

To ensure daily operations of the faculty functions correctly and reliably, the IT management group of the faculty must initiate and control the IT security strategies. Before formulating the strategies, it is critical to determine the likely risk that the faculty may encounter. Risk analysis is a process of determining those security risk and countermeasures upon which the faculty can formulate its information security strategy. The final outcome of this project will be a complete documentation which contains a guideline for FSKSM in designing and implementing a good security for IT system.

1.2 Background of the Problem

Faculty of Computer Science and Information System (FSKSM) which offer computer courses to faculty students as well as students from various faculties relies heavily on ICT to meet its operational academic activities. Every lecturer and even administrative support staffs are given a PC each. Each staff is responsible for the security of his or her

own PC. Academic assets such as exam results, exam questions, and lecture notes are kept electronically in lecturers' and/or administrators personal computers as well as in servers which are kept in various departments of the faculty. The personal computers and servers are networked and can be accessed within the faculty and therefore are vulnerable to attacks. Confidential information can be intercepted while traversing the network. A desperate student can compromise a computer system and change the information that is kept in computers or servers.

The faculty also maintains a few hundreds computers whereby different kinds of software are installed in them for the use of students. The security of these computers is also vulnerable as computer parts may be taken out by any passersby if the security of the lab is not taken seriously.

It is felt that many non-technically oriented staff may have potentially disastrous security vulnerabilities within their environment and not even realized it.

1.3 Statement of a Problem

To draft security guidelines that can be used by FSKSM staff to deter any security attacks so that academic assets can be protected from as much vulnerabilities as possible.

The issues that need to be addressed in implementing the research are:

i. What are academic assets that need to be protected?

ii. What are the threats and vulnerabilities associated with academic assets?

iii. What measures need to be taken to overcome the threats as well as vulnerabilities?

1.4 Importance of the Study

In summary, a major contribution of this research is a security guideline which can be followed by an individual in operating his or her PC. With this guideline, an individual who has access to this guideline will also be more aware of the security requirements in maintaining his academic assets. Furthermore, this guideline is not limited for use by FSKSM staffs but may also be used as a guidance by other individuals in securing their PCs.

1.5 Goal and Objectives

This project encompasses the following goals:

i. To protect the confidentiality, integrity and availability of academic assets.

ii. To produce security guidelines which can be used in the protection of academic information.

The objectives of the research are as follows:

i. To identify academic assets

ii. To identify vulnerabilities in IT environment of FSKSM

iii. To analyze security requirements for academic assets

iv. To disseminate security awareness amongst the staff of FSKSM

v. To draft appropriate security guidelines for protecting academic assets

1.6 Scope

The scope of the project is limited to the following:

i. The test bed is FSKSM

ii. Academic assets considered are limited to electronic academic data, computer software and hardware. It does not include assets which are not computer based such as furniture.

iii. The full cycle of risk analysis process is not carried out, however a survey of security requirements and awareness is conducted whereby the respondents are FSKSM lecturers, technicians and administrative staffs.

1.7 Contributions

The main contribution of this research is document for security guideline for academic assets. The document can be found in the Appendix. The research project managed to publish three papers as follows:

i. *Security Guidelines of Electronic Academic Assets*. Proceedings in MSTC 2002 Sept 19- 21 2002

ii. *Risk Analysis Guideline in IT Environment.* Proceedings in IT Symposium April,2000

iii. *Risk Analysis in IT Environment*. Seminar Penyelidikan FSKSM April 2000

The above published papers are described in chapters 2, 3 and 4 respectively.

CHAPTER 2

RISK ANALYSIS GUIDELINE FOR IT ENVIRONMENT

2.1 Abstract

An information security strategy needs to be tailored to meet an organization's specific requirements. Before formulating the strategies, it is critical to determine the likely risk that the organization may encounter. Risk analysis is a process of determining those security risk and countermeasures upon which the organization can formulate its information security strategy. This paper will present a comprehensive risk analysis guideline that can provide a framework for IT manager in designing and implementing a good security for IT system. By using this framework an effective balance between risk and rewards can be achieved. The concept of risk analysis and its significant in IT in will also be discussed.

Keyword: Information Technology Security, Risk, Vulnerabilities, Threat, Risk Management

2.2 Introduction

Nowadays most of the business organizations are becoming more dependence on computer in their day to day operations in processing information. This is due to the significant benefit provided by information technology that has drew a widespread of acceptance and approval from organizations worldwide. With the rapid growth of computer and networking technology, and the increase use of Internet, has made it feasible for any business organization to communicate with their counterpart globally. Unfortunately business information that flows through these open networks is vulnerable as it attracts unauthorized computer access.

Information, which is the key resource of any organizations, should be protected in order to advance the organization businesses and should therefore be regarded as an asset. The importance of such assets is usually expressed in terms of the consequential damage resulting from the manifestation of threats such as disclosure, improper modification, destruction or abuse of information. It can have adverse impact on the organization if the information's confidentiality, integrity and availability are violated and therefore it needs to be guarded against threats and attacks.

In order to reduce risk and encounter the loss of confidentiality, integrity and availability, an effective management of information security must be integrated within an organizations overall management plan. The management of information security is vital for the success of any organization.

2.3 Information Technology Security

Most companies use electronic information extensively to support their daily business processes. Organization's data such as customers, products, contracts, financial results and accounting are all stored in electronic form. It would be disastrous for any organizations if its electronic information were to become available to competitors or to become corrupted, false or disappear.

Continuity of operations and correct functioning of information systems is important to most businesses. Threats against computerized information and process are threats to business quality and effectiveness. The primary objective of information technology security is to put measures in placed which eliminate or reduce significant threats to an acceptable level. The confidence that may be held in the security provided by the information technology system is referred to as assurance. The greater the assurance, the greater the confidence that the system will protect its assets against the threat with an acceptable level of residual risk.

Security is the protection of information, systems and services against disasters, mistakes and manipulation so that the likelihood and impact of security incidents is minimized. Information technology security comprised of:

Confidentiality Sensitive business objects (information and processes) are disclosed only to authorized persons. Controls are required to restrict access to these objects.

Confidentiality threat can be manifested through access by unauthorized persons and authorized persons who have exceeded their privileges.

Integrity Business needs to control modification to objects (information and processes) from unauthorized access. Controls are required to ensure objects are accurate and complete.

Availability The need to have business objects (information and services) available when needed. Controls are required to ensure reliability of services. Availability threat is manifested through denial of service events, either physical in nature or logical such as computer viruses and intrusive software.

System risk is regarded as the likelihood of insufficient protection of information systems against certain kind of damaged or loss [1]. When organization managers are unaware of the full range of actions that they can take to reduce risk, subsequent plan to cope with system risk will less effective. This is why today damage and losses due to computer abuse and disasters are large and potentially devastating. Table 1, based on Datapro Research, give us an idea of what is going on in the real world. Also based on the same research findings, current employees of organization made up 81% of the total numbers of people that causes damage followed by outsider, 13%, and lastly former employees.

Table 1: Common Causes of Damage

Common Causes of Damage	Percentage
Human Error	52%
Dishonest people	10%
Technical Sabotage	10%
Fire	15%
Water	10%
Terrorism	3%

Security and risk management is tightly coupled with quality management. Security measures should be implemented in harmony with quality structures, processes and checklists. The value of information and processes should be known, the risks in the current environment analyzed, so that an appropriate set of countermeasures can be implemented. A cornerstone of countermeasures is risk analysis and the security policy.

2.4 Information Technology Security Life Cycle

Implementing security in information technology environment must follow six steps rotationally. The steps are risk analysis process, review security policy, identification of security requirements, mechanism selection, and monitor and review the existence security system [9]. However, this paper focuses on the processing of risk analysis.

2.5 Risk Analysis

Risk analysis is performed on system that has safety critical properties. It is a single most important safeguard an organization can provide for all its information systems. By employing risk analysis, an organization can save huge expenses by eliminating the basic weaknesses in information and communication systems. Therefore potential losses of information technology assets need to be identified and quantified [2].

Risk analysis can be defined as a process to ensure that security controls for a system are fully commensurate with its risks. It is an essential part of any security and risk management program. The analysis identifies the probable risk associated with vulnerabilities and provides the basis for establishing a cost-effective security program that eliminates or minimizes the effects of risks. In other words, risk analysis deals with [6]:

- Which assets need protection?
- What is the value of these assets?
- What threats prevail?
- What is the probability of each threat?
- What is the vulnerabilities of the assets to the threat?
- How much is the organization at risk?

Once all the risk has been identified, they need to be reduced to an acceptable, low level by inducing countermeasures. The output from risk analysis is the

summarization of risk assessment and it describe the general security risk management strategies as well as to give guidance on physical and administrative security controls. These security controls include:

i. maintain a high degree of integrity, availability and confidentiality of system and data;

ii. minimized potential abuse or misuse of system information technology assets;

iii. minimized harm or loss from accidental or malicious events to systems and data;

iv. maintain continuity of system operations.

There are several benefits resulted by performing risk analysis and among them are as follows:

i. Justification costs for additional security requirements can be generated with risk analysis that vindicating all security recommendations.

ii. Risk analysis programme can increase the productivity of the security or audit team

iii. Risk assessment should enable security to be driven into more areas and to become more devolved. It can allow security to become part of the organization's culture.

iv. Increased in security awareness among organization personnel.

v. With risk analysis, security can be properly targeted and related to the potential impacts, threats and existing vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure.

vi. Risk analysis can bring consistent and objective approach to all security reviews.

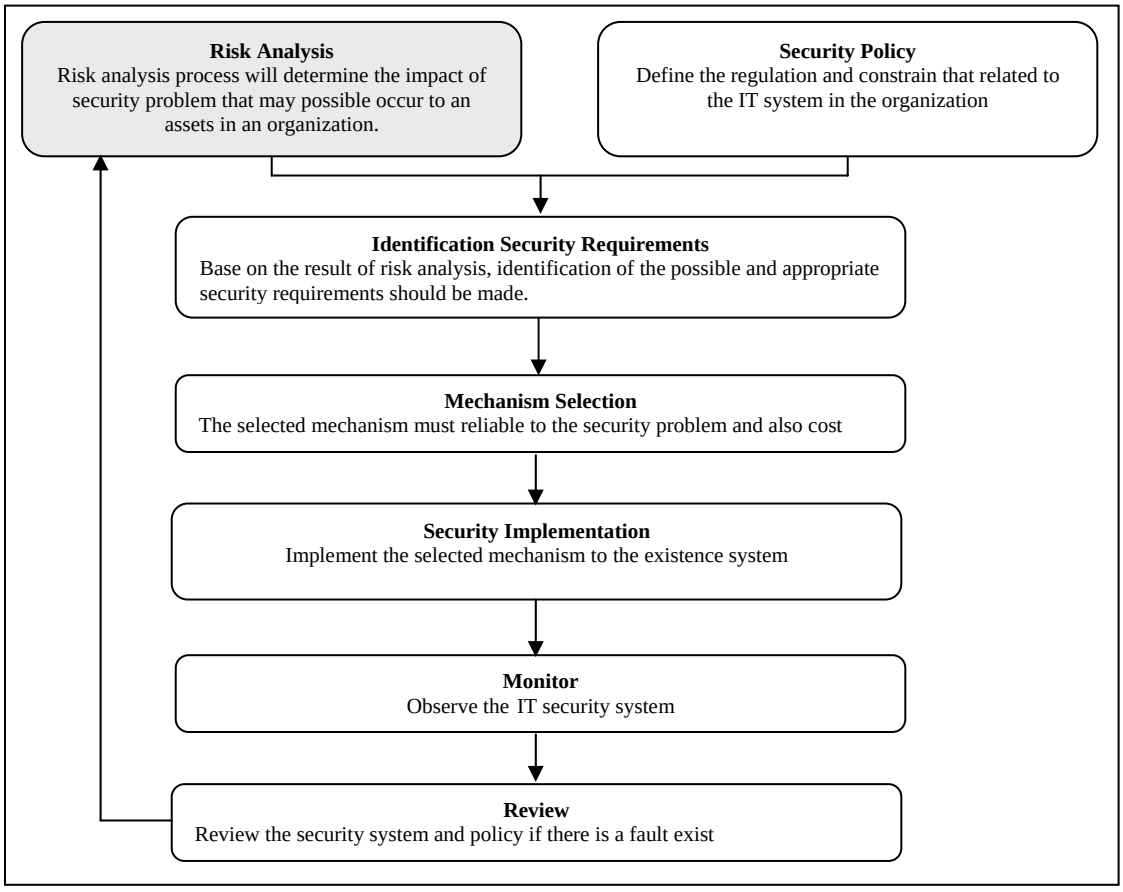

Figure 1: Information Technology Security Life Cycle

2.6 Risk Analysis Guidelines

Risk analysis is the quantification of risks and consists of risk identification, risk evaluation and accessing priority. The proposed guideline below is prepared for information technology managers to assist them in performing risk analysis effectively in their organization.

Guideline 1: Forming Risk Analysis Team

The most effective practice to accomplish risk analysis is through teamwork whereby each individual in the team represents each of the information technology disciplines. These disciplines include data processing management, system programming, system analysis, applications programming, data base administration, auditing, communication networks, system users and physical security. This is to ensure that the planning of the information security covers all aspects of the information technology management in the organization. Each of the individuals must be fully understand the flow of the organization operation in his/her department.

Guideline 2: Determine Assets at Risk

All organization's information assets must be identified and a checklist is prepared to document the collected data. These assets include application systems, databases, data files, documentation manuals, physical equipment, operating systems, computer hardware and related equipment and the continuity of the operations. From the checklist, classification of critical asset (confidential or sensitive) or otherwise is identified and this should be done by asking the owners of the information assets. The result of the process above is essential for determining the security control required for the information. Table 2 tabulate assets in information technology environment.

Guideline 3: Prioritize Critical Asset

It is not practical to identify the vulnerabilities and accessing the risk in a single comprehensive risk analysis. Instead asset should be prioritized whereby most critical assets is first accessed and continue with the assessment of less important assets.

Table 2: Asset in IT Environment

Asset	Examples
Data	Classified, tactical, operation, planning, financial, statistical, personnel, and logistic.
Communication	Communication equipment: lines, procedure, multiplexed, modem and LAN.
Hardware	Central machine (CPU, main memory, I/O channel), storage medium (hard disk, diskettes, paper printout), special interface equipment (database machine, network front-end), I/O devices (printer, terminals), microcomputer.
Software	Operation system and programs: application, standard application, test programs, communication, and microcomputer.
Personnel	Computer personnel: system analyst, programmers, security officer, temporary employee.
Physical	Environmental system (air conditioning, power, water, lighting), building (computer rooms, data preparation area).

Generally, the highest priority should be assigned to information assets that are most critical in organization operations. Next priority is assigned to assets where data confidentiality or disclosure and dissemination are the controlling factors while third priority is assigned to assets that are sensitive. Finally, all information assets are assigned to lower priority.

Guideline 4: Identify Risk Analysis Approach

The principal step in the entire risk analysis process is identifying risk analysis methodology. The analytical process analyzes the relationships between assets, threats, vulnerabilities and/or safeguards and possibly other element. The outcome of the analysis is to determine potential losses that result from harmful events.

Risk analysis methodology should provide the mechanism to compare possible losses to the organization with the cost of security safeguard designed to protect against the losses. The outcome of the analysis would be a quantitative statement of the impact of a risk or the effect of specific security problem. The two key elements in risk analysis are:

i. a statement of impact or the course of a specific difficulty if it happens.
ii. a statement of the probability of encountering that difficulty within a specific period of time.

An approach is required so that the work of risk analysis could focuses on security effort where it is needed and enables a cost and time effective approach. It is neither resource or time effective to conduct detailed reviews for all systems, nor it is effective not to address serious risks. An approach that provides a balance between these extremes involves conducting high reviews to determine information technology security needs of the systems that analyze to a depth consistent with these needs. There are four types of approach, basically baseline approach, informal approach, detailed risk analysis and combine approach [4]. Table 3 tabulates the advantages and the disadvantages of each approach.

It is highly recommended for majority of organizations to apply the hybrid approach in analyzing risk.

Table 3: Approaches in Risk Analysis

Approach	Advantages	Disadvantages
Baseline	- No significant resources are needed for detailed risk analysis. - Time and effort spent on safeguard selection is reduced. - Similar baseline safeguards can be adapted for any systems that are operated in the same environment.	- Too expensive or too restrictive security for some systems if the baseline level is set too high but it is set too low, then there might be not enough security for some systems - Difficulties in managing security relevant changes.
Informal	- No additional skills need to be learned to do the analysis. - Performed quicker than detailed risk analysis.	- Likelihood of missing some risks since it is done without a structure approach. - Result may be influenced by subjective views due to the informality of the approach. - Very little justification for the safeguard selected. - Difficult to manage security relevant changes without repeated views.
Detailed Risk Analysis	- Security level is identified appropriated to the security needs of each system. - Ease of managing security.	- Consumes considerable amount of time, effort and expertise.
Hybrid	- Use simple high level approach to collect the necessary information before significant resources are committed. - Possible to build an immediate strategic picture of the organizational security programme. - Resources and money can be applied where they will be most beneficial - Systems that are likely to be at high risk can be addressed early.	- If high level risk analysis leads to inaccurate results, some systems might not be addressed.

Guideline 5: Identify Vulnerabilities and Threats

According to FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, vulnerabilities is defines as a weakness that might be exploited to cause harm or loss. It is often analyzed in terms of missing safeguard and can cause risk to a system because they may allow a threat to harm the system. There are several categories of vulnerabilities that may impact an information system. This is shown in Table 4.

Vulnerabilities and potential risk that are associated with each asset in the asset checklist must be identified and categorized in terms of:

- Accidental acts such as errors, disclosure, modification and negligence.
- Intentional acts such as theft, extortion, physical sabotage and wire tapping.
- Natural catastrophe such as water, fire and tornadoes.
- Interruption of utility such as electricity and communications.

Guideline 6: Calculation of Risk and Balancing Losses

The estimated value of potential losses and the probability of occurrence of a threat are used for the definition of risk [5]. In simple form, the calculation is done based on the formula [10]:

Risk = Loss Estimate × Probability of Occurrence

Risk analysis presumes that the cost of controlling any risk should not exceed the maximum loss associated with the risk. To arrive at cost-effective security solutions, risk analysis requires identify probable loss or quantifying the value of an item to the organization.

Table 4: Vulnerabilities of IT System

Vulnerabilities	Examples	Threats
Software	- Inadequate configuration management that permits program errors - Unauthorized automated routines - Inadequacies in system and application software	- May result in processing or calculation errors, - May allow unauthorized access to hardware, data or programs
Hardware	- Improper operation of hardware - Lack of proper hardware maintenance - Inadequate physical security - Inadequate protection against natural disaster	- Hardware malfunction or damage result in denial of service - Unauthorized access to hardware leading to hardware theft, abuse, misuse, damage or destruction.
Data	- Inadequate access control	- Unauthorized access or authorized personnel to exceed privileges with the potential result of both accidental and malicious deletion, corruption, modification and destruction of data.
Administrative	- Weaknesses in effective administrative control of IT resources - Inadequate or nonexistence administrative and security policies, guidelines, training and controls	- Unauthorized access of sensitive data - Direct file or program modification
Communication	- Inadequate access control - Inadequate measures to prevent circuit failure from both natural disaster and human activities.	- Unauthorized access to networks - Transmission interception
Personnel (insiders)	- Inadequate physical and logical controls - Inadequate administrative procedures to minimized or detect accidents involving IT resources	- Access to systems by insiders which is beyond his privileges - Theft, abuse, misuse, damage or destruction of IT resources
Facility	- Inadequate physical security - Inadequate protection against natural disaster	- Unauthorized access that may lead to facility and content misuse, damage, theft or destruction

Using the list of vulnerabilities associated with the organization's information assets, identify the risk associated with each threat. Next, determine the potential economic impact of those risks or events. Then, estimate the probability of the undesirable events within a specified period of time.

2.7 Conclusion

Information is the one of the important assets in any organization that is related to information technology. Therefore the security of this assets must be realized and need to be integrated in the operations of the business. However, the process to determine which security controls are appropriate and cost effective, are quite often a complex and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this process onto a more objective basis whereby it provides an organization with a means of assessing the risk that might threaten the security of the organization.

Risk analysis is a vital part of any organization's risk management program. It is not a task to be accomplished once for all time. The risk analysis process should be conducted with sufficient regularity to ensure a realistic response to the current risks associated with its information assets.

2.8 References

1. Straub, D.W. and Welke, R.J. “Coping with System Risk: Security Planning Models for Management Decision Making”. MIS Quarterly; Minneapolis, Dec 1998.
2. Badenhorst, K.P. and Eloff, Jan H.P. “Computer Security Methodology. Risk Analysis and Project Definition”. Computer and Security vol 9, pg 339 – 346, Jun 1990.
3. Lane, V.P. Security of Computer Based Information Systems. Macmillan Education Ltd, 1988.
4. Guidelines for the Management of IT Security – Part 2: Managing and Planning IT Security. ISO/IEC TR 13335-2, 1997.
5. Friedl, W.J. “The Computer Security Framework”. Journal IEEE, 1990, pg 93 - 99.
6. Halliday, S., Badenhorst, K. and Solms, R.V. “A business Approach to Effective Information Technology Risk Analysis and Management”. Information Management & Computer Security, 1996, pg 19 –31.
7. Charles P.Pfleeger, Security In Computing, Prentice Hall: United State, 1989.Charlie Kaufman, Radia Perlman, Mike SpecinerNetwork Security Private Communication in a Public World , Prentice Hall: United State, 1995.
8. D.W. Roberts. Computer Security Policy, Planning and Practice, Blenheim Online: London, 1990.

9. KK. Wong. Risk Analysis and Control A Guide for the Department Manager, The National Computing Center Limited, UK, 1977.

CHAPTER 3

RISK ANALYSIS IN IT ENVIRONMENT: A CASE STUDY OF FSKSM

3.1 Abstract

The management of information security is vital for the success of any organization. In order to reduce risk and encounter the loss of confidentiality, integrity and availability, an effective management of information security must be integrated within an organizations overall management plan. Faculty of Computer Science and Information System (FSKSM) relies heavily on computer systems to meet its operational requirements. These computer systems, related data files and the information derived from them are important assets of the faculty. To ensure daily operations of the faculty function correctly and reliably, the IT management group of the faculty must initiate and control the IT security strategies. Before formulating the strategies, it is critical to determine the likely risk that the faculty may encounter. Risk analysis is a process of determining those security risk and countermeasures upon which the faculty can formulate its information security strategy. The final outcome of this project will be a complete documentation

which contains a policy and guidelines for FSKSM in designing and implementing a good security for IT system.

Keyword: Information Technology Security, Risk Analysis

3.2 Introduction

In the modern world of information and communication, administrative tasks, both public and industry, are increasingly supported by the use of information technology (IT). Numerous work processes are electronically controlled and large amounts of information are stored as digital data, electronically processed and transferred through local and public networks. Some public or commercial tasks are not possible without IT, others only utilized it partially. As a result, many organizations, in both administration and industry, depend on an efficient IT operation. It is only possible for authorities and companies to reach their goals if IT systems function correctly and reliably.

IT security is to be seen as an integral part of the primary task that is carried out by any organizations. However, most organizations put security issues in a low priority. This paper will highlight the importance of IT security management, the responsibility for the secure and correct fulfillment of IT tasks must be delegated in the same way as the responsibility for the primary task itself. As in the case with the primary task, the ultimate responsibility for IT security rests with the management. The corporate tasks required for

IT security, the organization, delegation of responsibilities and the necessary controls should be coordinated by a specially established organizational unit, the IT Security Management Team.

3.3 Objectives

The objectives of the research are as follows:

vi. To identify vulnerabilities in IT environment of FSKSM

vii. To explore the techniques for conducting risk analysis that is suitable for IT environment in FSKSM

viii. To design appropriate security solutions for FSKSM

3.4 Scope

The scope of the project comprises of:

i. Risk analysis that would cover the security needs of FSKSM by referring to an international standard methodology

ii. A survey of risk analysis technique. Based on this survey, a relevant risk analysis method will be applied in the FSKSM IT environment.

3.5 Fundamental Information Technology Security

Today, most of the business organizations are becoming more dependent on computer in their day to day operations in processing information. This is due to the significant benefit provided by information technology that has drew a widespread acceptance and approval from organizations worldwide. With the rapid growth of computer and networking technology, and the increase use of Internet, it is feasible for any business organization to communicate with their counterpart globally. Unfortunately, business information that flows through these open networks is vulnerable as it attracts unauthorized computer access. Due to this, the internal IT system in an organization should be controlled by a security management system. In the following sections, we will describe a fundamental IT security concept and process which related to this project.

Security is the protection of information, systems and services against disasters, mistakes and manipulation so that the likelihood and impact of security incidents is minimized. Information technology security comprised of:

Confidentiality Sensitive business objects (information and processes) are disclosed only to authorized persons. Controls are required to restrict access to these objects. Confidentiality threat can be manifested through access by unauthorized persons and authorized persons who have exceeded their privileges.

Integrity Business needs to control modification to objects (information and processes) from unauthorized access. Controls are required to ensure objects are accurate and complete.

Availability The need to have business objects (information and services) available when needed. Controls are required to ensure reliability of services. Availability threat is manifested through denial of service events, either physical in nature or logical such as computer viruses and intrusive software.

IT security system can be categorized into several categories which are data security, software security, hardware security, network security and physical security. The system can be implemented based on certified standard, policy and guidelines.

3.6 Information Technology Security Action Plan

To ensure that IT functions correctly and reliably, a systematic approach must be taken which leads to an integral and complete result. In order to attain the required objective of "adequate and appropriate IT security", an effective action plan is recommended to the organization management. The responsibility of a successful implementation of this action plan must be dealt by the management group in an organization. The implementation must refer to the IT control and security action plan as shown in Figure-

1. The IT security action plan needs to be tailored with the current security policy and standard.

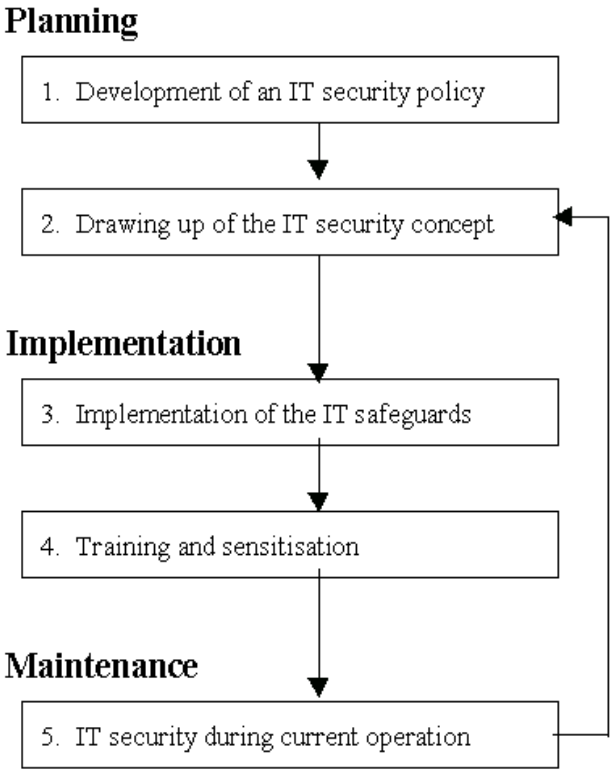

Figure 1: Information Technology Security Action Plan

3.6.1 IT Security Policy

According to Pottas and Solms,

> *"IT security policy is a document stating high-level, global organizational security objectives. This document must be compiled on a managerial level to ensure commitment and support from management".*

The fundamental goal of IT security policy is to communicate to everyone in the organization, that information is a valuable asset to the corporation and that everyone is responsible and accountable for protecting it. The IT security policy is a visible representation of security considerations, requirements, priorities, assumptions, and responsibilities. It also demonstrates management commitment to protect corporate information. It identifies clearly what information must be protected, who must protect it, and how it must be protected. It states legally defensible requirements for employee conduct and responsibilities and the consequences for misuse of these resources. The policy consists with:

- States clearly what corporate information must be protected
- Establishes unambiguous responsibilities for protecting information assets
- Sets clear expectations of privacy in the workplace
- Defines an acceptable behavior
- Limits exposure to liability
- Supports the organization's mission and goals
- Guides selection of information technology and facilitates proper implementation
- Facilitates establishment of security incident prevention and response programs

3.6.2 Security Standard

Implementing IT security system in an organization must refer to the standard that produced by certified organization such as ISO (International Standard Organization),

British Standard Institution, Department of Defence (DoD US) and Canadian Institute. The IT security standard is a set of requirements which describes a minimum proficiency level with which information security countermeasures or product must comply. The standard must cover all aspects of IT operations such as management, technical, operation, policy and procedure.

Based on the literature review, current security standards used by most IT organization are:

- British Standard 7799
- International Standard (IS) (IS) 15408/C.C Version 2.1
- Australian Standard 4444
- Common Criteria - Orange Book
- Common Criteria – red book

3.7 Information Technology Security Life Cycle

IT security system can be implemented by following the six steps rotationally which are risk analysis process, security policy review, security requirements identification, mechanism selection, and the existing security system monitoring and reviewing as shown in Figure-2. In this research we will only focus on the process of risk analysis.

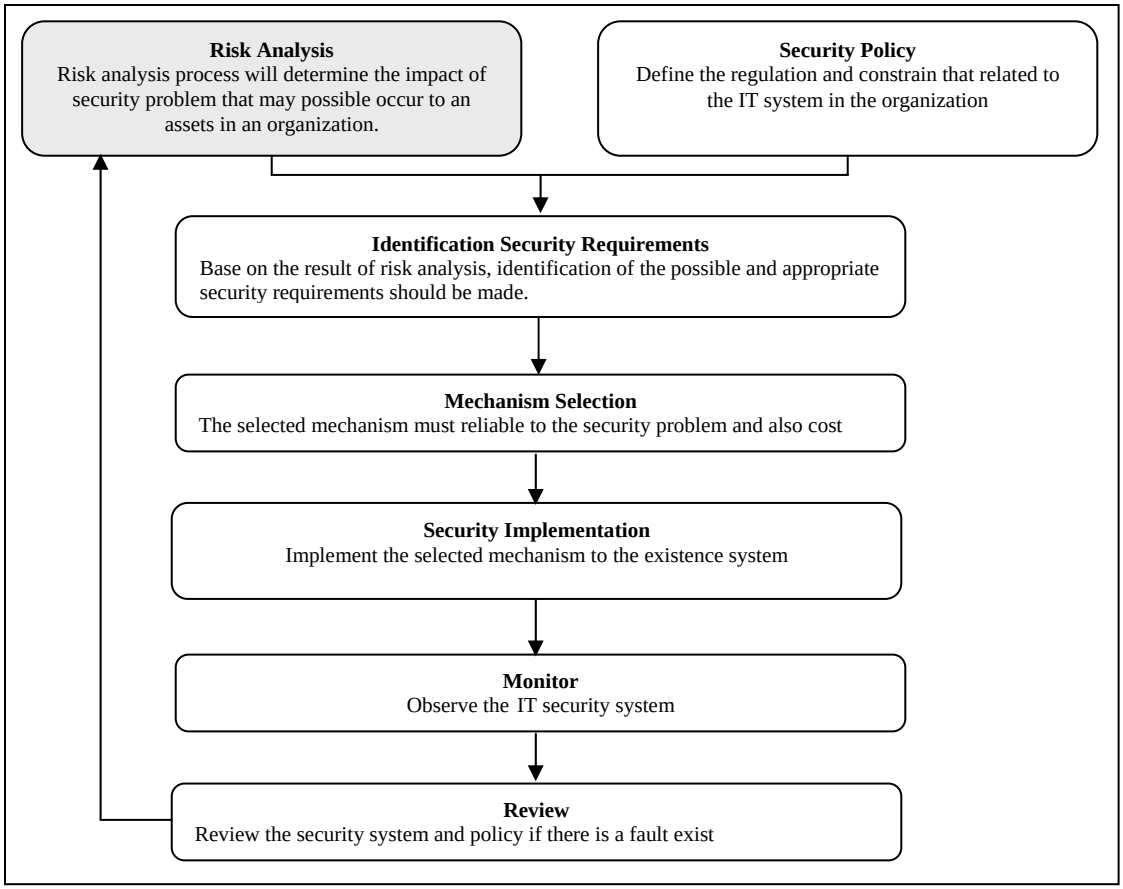

Figure 2: Information Technology Security Life Cycle

3.8 Risk Analysis for FSKSM

Risk analysis forms the basis for establishing a cost-effective risk management program. Risk management ensures that reasonable steps have been taken to prevent situations that can interfere with accomplishing the organization's mission. Managing information security within FSKSM requires commitment and support on the part of executive, technical, program management (head of departments) and supporting staffs. Employees may recognize the need for information security and risk management but normally

attach an importance to it in accordance with the interest and emphasis demonstrated toward it by the management. Faculty management should be involved in the risk analysis process and, in the development and implementation of a security plan.

Risk analysis is performed on system that has security critical properties. It is a single most important safeguard an organization can provide for all its information systems. By employing risk analysis, an organization can save huge expenses by having a safety net that can overcome threats to information and communication systems. In order to reduce potential losses of information technology, assets need to be identified and quantified.

Risk analysis can be defined as a process to ensure that security controls for a system are fully commensurate with its risks. It is an essential part of any security and risk management program. The analysis identifies the probable risk associated with vulnerabilities and provides the basis for establishing a cost-effective security program that eliminates or minimizes the effect of risks. In other words, risk analysis deals with

- Which assets need protection?
- What is the value of these assets?
- What threats prevail?
- What is the probability of each threat?
- What are the vulnerabilities of the assets to the threat?
- How much is the organization at risk?

Once all the risk has been identified, they need to be reduced to an acceptable, low level by inducing countermeasures. The output from risk analysis is the summarization of risk assessment and it describes the general security risk management strategies as well as to give guidance on physical and administrative security controls.

3.9 Expected Result and Achievement

At this moment, there are several IT systems that are being used in FSKSM, for example staffs' attendance and inventory. In this project, a security critical IT system of the faculty will be identified for assessing the risk. The outcome of the analysis will be a documentation that contains policy and guidelines in designing and implementing a good security for the chosen IT system. The design of a risk analysis guideline for IT environment is in progress. A related paper on this guideline entitled *"Risk Analysis Guideline in IT Environment"* was presented in April, 2000 at IT Symposium Universiti Kebangsaan Malaysia.

An effective IT security solution for FSKSM is based on the proper process of risk analysis and supported by establish security policy and standard. Due to that, a deep research on risk analysis and IT security should be made in order to produce a complete set of documented security solution. The operational framework of the research group is given in the Figure-3.

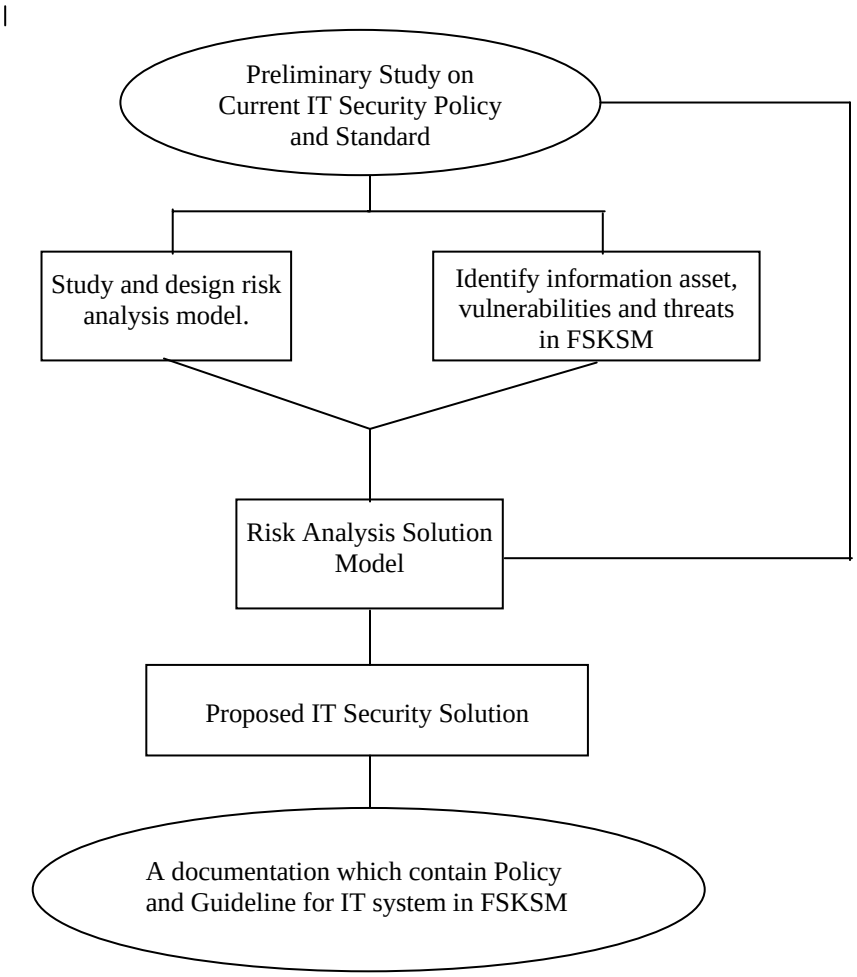

Figure-3: Operational Framework

3.10 Reference

1. Straub, D.W. and Welke, R.J. “Coping with System Risk: Security Planning Models for Management Decision Making”. MIS Quarterly; Minneapolis, Dec 1998.

2. Badenhorst, K.P. and Eloff, Jan H.P. " Computer Security Methodology. Risk Analysis and Project Definition". Computer and Security vol 9, pg 339 – 346, Jun 1990.

3. Lane, V.P. Security of Computer Based Information Systems. Macmillan Education Ltd, 1988.

4. Guidelines for the Management of IT Security – Part 2: Managing and Planning IT Security. ISO/IEC TR 13335-2, 1997.

5. Friedl, W.J. "The Computer Security Framework". Journal IEEE, 1990, pg 93 - 99.

6. Halliday, S., Badenhorst, K. and Solms, R.V. "A business Approach to Effective Information Technology Risk Analysis and Management". Information Management & Computer Security, 1996, pg 19 –31.

7. Charles P.Pfleeger, Security In Computing, Prentice Hall: United State, 1989.

8. D.W. Roberts. Computer Security Policy, Planning and Practice, Blenheim Online: London, 1990.

9. Pottas. D and Solms S.H. Superceding Manual Generation of Access Control Specisication – From Policies to Profiles, Computer Security, 1993.

10. A Guide to Effective Business Continuity in Support of the Year 2000 Challenge. October 14, 1998

CHAPTER 4

SECURITY GUIDELINES OF ELECTRONIC ACADEMIC ASSETS

4.1 Abstract

As the country moves into the Information Age, the use of Information and Communication Technology (ICT) has become a ubiquitous activity in university departments for academic and administrative purposes. University academic information resources are valuable assets and the security of these assets should be managed properly so that these information resources can be accessible when and where it is needed. Without proper security measures and controls may result in the compromise, improper modification, or destruction of the information resources.

This paper addresses security issues in the context of electronic academic assets. Threats and vulnerabilities of academic assets are discussed. Assets, threats and vulnerabilities of academic information resources are determined through a risk analysis approach, whereby a survey is conducted amongst academic staffs as

respondents. Security controls that can be employed to reduce the risks of attacks on these assets are then determined. The final outcome of the research is a security guideline that may be followed by academic staffs and others who are responsible for the security of electronic information in a university environment. The guideline addresses issues such as choosing good passwords, preventing virus attacks, e-mail security, pc intrusion and administrative responsibilities. It defines the security responsibilities of both the users and the administrators who manage computers and networks.

With the availability of security guideline and proper training to staffs who managed academic assets, the security of academic assets can be enhanced and the network in the academic environment as a whole gains more trusts.

Keyword: Risk Analysis, Computer Security, Security Guideline

4.2 Introduction

Today, computer usage has become more pervasive in most activities carried out by organizations. This is due to the significant benefit provided by information technology that has drew a widespread acceptance and approval from organizations worldwide. With the rapid growth of computer and networking technology, and the increase use of Internet, it is feasible for any business organization to communicate with their

counterpart globally. Unfortunately, information that flows through these open networks is vulnerable as it attracts unauthorized computer access. Applications that employ ICT are also more vulnerable to threats such as virus attacks, intrusions and denial of service. Confidential information can be intercepted while traversing through the network. In 2001 alone, some 52,000 attacks on computer network were reported to a Carnegie Mellon University center that coordinates computer emergency responses [1]. Due to this, the internal IT system in an organization should be controlled by a security management system.

Academic institutions have been using computers for several decades. More and more applications are being employed such as students' registration, students' records and staff payrolls to enhance the efficiency of daily activity in the institutions. In addition, the use of internet has grown exponentially in many campuses, hence the emerging of campus-wide on-line applications. Most communications amongst staffs are done through e-mail, e-learning applications are developed to provide easy access to lecture notes to students and students use campus network to access information related to their course work on sites around the world [2]. Therefore measures to secure academic information and services are very important since the compromise of this information and services can affect the running activity, the credibility of the university as well as students' future.

In this paper we discuss security issues in academic assets and suggests some security guidelines for managing it. An analysis of what assets to protect and what to

protect it from is carried out at *Fakulti Sains Komputer dan Sistem Maklumat* (FSKSM) by using risk analysis technique as a guidance. Security guidelines are then drafted based on several standard security policies and guidelines.

4.3 Security Issues in Electronic Academic Assets

Academic assets play an important role in academic institutions. Since academic institutions run their daily activities by using ICT, most of theses assets are kept electronically. The vulnerabilities of electronic assets are different from paper-based assets. When paper-based assets are stolen, the assets are no longer available. Keeping information is different; stealing information usually just obtains access to the computers containing it and copies or otherwise uses it without permission. The information is still available, but the value of information may have been reduced [3]. Therefore security aspects should be considered when managing electronic academic assets.

Security issues that need to be considered when managing academic assets are [4]:

i. Confidentiality – The assurance that information is not disclosed to unauthorized users.
ii. Integrity – The assurance that the information is not modified or corrupted.
iii. Availability – The assurance that information is readily available when needed.

Table 1 summarizes security issues of academic assets.

Table 1: Security Issues of Academic Assets

Types	**Examples**	**Security Issues**
Administrative documents	Procurements, strategic plans reports	Availability, confidentiality, integrity
Software	Programming languages and applications	Availability, integrity
Databases	Students records, staff records	Availability, confidentiality, integrity
Academic staff	lecture notes, questions banks , publications	Availability, confidentiality, integrity

Academic staffs use personal computers (PC) for both research and teaching activities. They prepare their lecture notes using PC and keep examination questions and students results in the hard disk of their PCs. Research findings and publications are also kept in the hard disks. Sometimes staffs attach confidential data such as examination questions and results along with e-mail messages to their colleagues.

The three security issues can overlap, and they can even be mutually exclusive, for example, strong protection of confidentiality can severely restrict availability. These three properties are largely independent but sometimes overlapping as shown in Figure 1 [4].

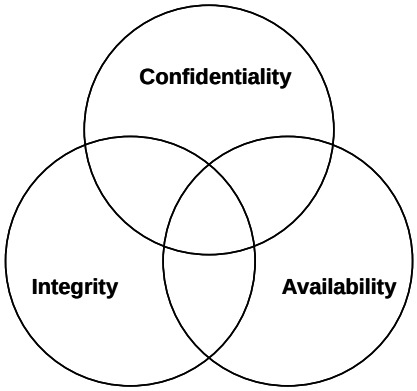

Figure 1: Relationship between security goals

4.4 Methodology

In order to come out with the security guideline that is suitable for FSKSM, an analysis of what assets to protect and what to protect it from is carried out by using risk analysis technique as a guidance. Figure 2 describes the framework that is used to draft the guideline. Information is acquired from lecturers, support staffs and technicians through questionnaires. The survey is conducted for identifying the risks incurred by the respondents in personal computer usage and their security awareness. It includes managing their data files, dealing with threats such as virus, PC intrusion and hardware theft, and software usage. From the analysis of the questionnaire, the security awareness and security practices amongst staffs are determined. It is found that the staffs are aware of security requirements, however they lack security practices.

.

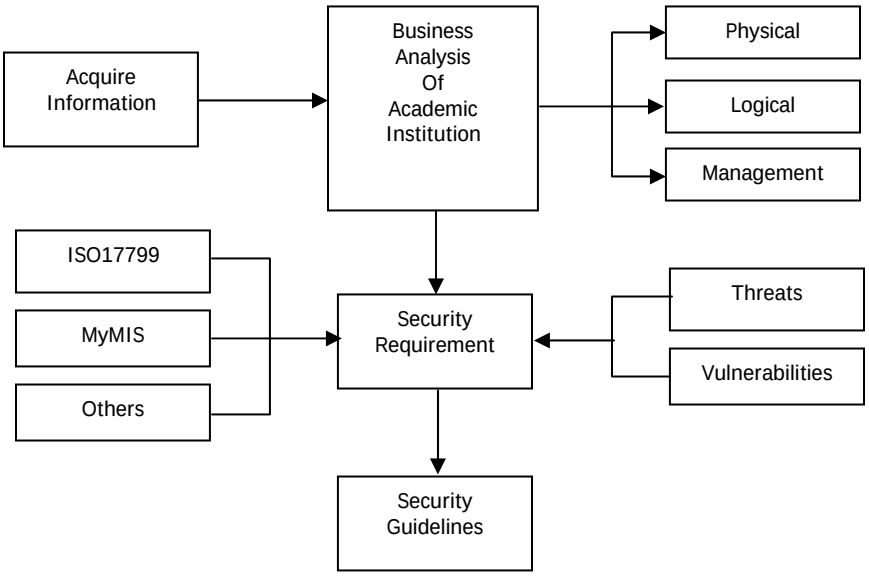

Figure 2: Operational Framework for Drafting Security Guidelines

Based on responses from the survey and references from security policy standards, such as ISO17799, MyMIS and security policy and guidelines from other organizations [5 - 8].

4.5 Security Guidelines

The use of ICT has expanded across academic institutions, whereby it has been utilized in most academic applications. Due to this, there is a growing concern on the security of the publicly available of electronic information. This project is carried out to address this issue.

Security guidelines are typically a collection of system-specific of procedural-specific suggestions for best practices. They are not requirements to be met but are strongly recommended. Security guidelines are different from security policies. Typically, a policy is a document that outlines specific requirements or rules that must be met. Security guidelines should reflect the organizational information security policy. Some policies that have been drafted omit security guidelines [9].

The security guidelines for academic assets are drafted with the following objectives:

i. Raise awareness of security threats in the use of ICT for academic purposes.
ii. Provide measures to reduce the security threats.
iii. Serve as a starting point for developing security guideline for academic environment.
iv. Create a ground framework to assist in developing the security policy for the academic institutions.

The guideline is to provide guidance, not solutions on managing the security of electronic academic information resources. This guideline is classified into several categories:

i. Password
ii. Virus Attack
iii. E-mail Security
iv. PC Intrusion
v. Administrative Responsibility

vi. General Security Recommendations

Each category is organized by first explaining the vulnerabilities or threats if measures are not taken. It then lists security measures that can taken in an attempt to reduce the probability of exploitation of vulnerability. This measure may take one of many forms: an operational procedure, a software security feature such as anti-virus and firewall, the use of encryption, and several others. Table 2 summarizes measures listed in each category.

Table 2: Summary of Security Guidelines Document

Category	**Descriptions**
Password	Criteria for choosing good passwords
	Password Usage
	Password Protection
Virus	Reducing Virus Infections
E-Mail	Reducing threats through e-mail
PC Intrusion	Avoiding PC Intrusion
Administrative Responsibilities	Securing the network
General Security Recommendations	Good security practices
	Ethics to be abide
	Security awareness training

The full documentation of the security guidelines is documented in Recommended Security Guidelines for Academic Assets in FSKSM.

4.6 Conclusion

The security guidelines address issues such as choosing good password, preventing virus attacks and pc intrusion. It defines the security responsibilities of both the users and the people who maintain computers and networks in the faculty. The guideline drafted can also be used by individuals who manage electronic information.

Security guidelines are good security practices for protecting electronic academic assets in order to reduce risk and encounter the loss of confidentiality, integrity and availability. To achieve the goal, the guidelines must be simple and short enough so that it is easy to understand and follow by all levels of staffs. Besides this, to ensure that the practices are carried out by all staffs, an effective management of information security must be integrated within an organization's overall management plan.

The security guideline formulated can be used as a starting point in drafting security policy. With the application of security policy in the academic environment, the security of academic assets can be enhanced and the network as a whole can be trusted.

4.7 Reference

1. Holsendolph, E., 2002. "Hackers vs. colleges: Security Bolstered for University Computer Systems", Cox News Service.
2. ITATF Security Working Group, 1998. "Improving Network and Computer Security at the University of California", Berkeley, Report of the ITATF Security Working Group.
3. Cramer, M.L., 1997. "Measuring the Value of Information", Information Warfare Conference 1997, Vienna, Virginia.
4. Mohd Aizaini Maarof, Subariah Ibrahim, Mazleena Salleh, "ICT: Security Issues To Be Pondered", Proceedings in International Conference of Education and ICT, October 2000.
5. Engelman, N., "Developing an Anti-Virus Security Policy", Cybec Pty Ltd, Available Online http://www.vet.com.au/html/vvcc/anti-virus/
6. NSW Government Agencies, 2001. "Information Security Guidelines for NSW Government Agencies".
7. BFB IS-3 Information Security, 1998. "Business & Finance Bulletin IS-3, Electronic Information Security, University of California.
8. ITATF Security Working Group, 1998. "Improving Network and Computer Security at the University of California, Berkeley".

9. Siponen, M.T., 2000. “Policies for Construction of Information Systems’ Security Guidelines”, 16th Annual Working Conference on Information Security, Beijing, China.

CHAPTER 5

CONCLUSION

5.1 GENERAL CONCLUSION

The use of ICT in UTM has increased significantly in the past few years. In responds to this, there is a need for security awareness among the staffs since each staff has to manage his or her own PC. Therefore it is necessary to have Guidelines of Electronic Academic Assets that can be followed by the staff. Some guidelines are not limited to FSKSM staff only but can be used by any individual who maintain a PC. They can review the guidelines and pick any that are applicable to their situations. There are no systems that are completely secure, however the best that can be done is to obtain an acceptable level of security and to proceed with the understanding that new threats will always exist.

5.2 RECOMMENDED GUIDELINES

The faculty management needs to provide a security awareness training program to all staffs in order to support faculty's efforts to maintain secure academic assets. In addition, there should be regular reminders of security threats and solutions by IT administrators. Further research related to security plan and policy should be carried out in order to implement the IT Security Policy in the UTM. These include hardware and software security, proper physical, procedural, and personnel access controls. Guidelines stated in this document can be used as a starting point in drafting the policy. The security plan and policy should carry out the whole process of risk analysis and must be revised periodically as computer technology keeps on changing.

APPENDIX

Recommended Guidelines of Electronic Academic Assets

Subariah Ibrahim[1]
Mazleena Salleh[2]

Faculty of Computer Science and Information System
University Technology Malaysia

[1]subariah@fsksm.utm.my [2]mazleena@fsksm.utm.my

Abstract

As the country moves into the Information Age, government agencies including universities are revolutionizing the way they operate. Computer system has become a part of their staff office equipment and most of the information kept is in the electronic form. To make this information useful, it must be accessible when and where it is needed. Now the world trend is towards global interconnectedness and Internet connectivity makes it feasible for information to be available globally.

However, managing electronic data as well as connectivity without employing any security measures and controls can result in the compromise, improper modification, or destruction of the information. Disclosure of sensitive information to the wrong hands can ruin and destroy businesses, corporate agency or government.

This guideline provides security guidelines to academic staff in the university, and to others who are responsible for the security of electronic information in a university environment. The objective of this guideline is to address issues in the context of protecting electronic academic assets. It discusses some of the threats and vulnerabilities of these academic assets, and some of the security controls that can be employed to reduce the risks.

1.0 Introduction

Information and Communication Technology (ICT) has become a necessary tool in academic institution, may it be in management as well as in teaching. However the use of ICT comes with commensurate risks, such as compromise of confidential assets, loss of information accuracy or integrity and interruption of services. Therefore measures to secure academic information and services are very important since the compromise of this information and services can affect the running activity, the credibility of the university as well as students' future.

Universiti Teknologi Malaysia provides a personal computer for each academic staff so that ICT can be employed in their academic activities. Each individual staff cannot rely on measures taken by IT staff to protect his/her resources, but each staff should take some responsibility in protecting the academic assets under his/her domain. To this date, there is no security guideline or policy that can be followed by the staffs to minimize the risks while using their PCs. This guideline offers several measures or suggestions for best practice that can be taken by individual staff in securing his/her academic assets.

In this guideline academic assets includes lecture notes, examination, tests and quizzes questions, examination results, publications and research findings.

2.0 Scope

The purpose of this document is to provide guidance, not solutions on managing the security of electronic academic information resources. This guideline is intended for use by FSKSM staff in maintaining the academic assets but does not apply to information such as student and staff records that are kept in the mainframe computer under the management of Pusat Komputer. Some parts in the document may be applicable to any individual who maintains a PC.

3.0 Aim

The aims of this Guideline are to:

i. Raise awareness of security threats in the use of ICT for academic purposes.
ii. Provide measures to reduce the security threats.
iii. Serve as a starting point for developing security guideline for academic environment.
iv. Create a ground framework to assist in developing the security policy for the university.

4.0 Guideline Organization

A security measure is a step that is taken in an attempt to reduce the probability of exploitation of vulnerability. This measure may take one of many forms: an operational procedure, a software security feature such as anti-virus and firewall, the use of encryption, and several others.

This guideline is classified into several categories:

i. Password (Section 5.1)
ii. Virus Attack (Section 5.2)
iii. E-mail Security (Section 5.3)
iv. PC Intrusion (Section 5.4)
v. Administrative Responsibility (Section 5.5)
vi. General Security Recommendations (Section 5.6)

5.0 Recommended Guidelines for Electronic Academic Assets

It is important to note that no PC can ever be completely secure, what more if it is connected to the network. However by following the guideline outlines in this document may reduce the extent of security risks. This guideline presents potential security problems and outlines measures to reduce the threats.

5.1 Password

Password is one of the mechanisms available for authentication in order to protect the resources kept in a computer system. Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Users' passwords are normally kept in a file which will be used by the operating system to validate the user who log-in to a computer system. Hackers often use little-known vulnerabilities in computers to steal password files even when it is encrypted. They then use password-cracking programs that can discover weak passwords within password files. Once a weak password is discovered, the hacker can enter the computer as a normal user and use a variety of tricks to gain complete control of the computer and the network.

5.1.1 Choosing a Password

If simple or weak passwords are used, it will be easy to guess it. Therefore the object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about the chosen password. This leaves him no alternative but a brute-force search. A search of this sort, even conducted on a machine that could try one

million passwords per second would require, on the average, over one hundred years determining the correct password.

Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

The criteria for selecting good passwords are as follows [1]:

i. Minimum length of eight (8) alphanumeric characters.
ii. Contain a combination of letters (such as, a-z, A-Z), numbers, or other displayable special characters (such as, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
iii. Avoid words that can be found in dictionary, that is not a word in any language, slang, dialect, jargon, etc. (such as RAHSIA, PASSWORD, ADIKADIBRA)
iv. Do not use more than three consecutive characters in any position from the previous password.
v. Do not use passwords that exhibits obvious patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
vi. Do not use the user ID or personal information such as family names, birthdays, addresses and phone numbers as part of the password (such as Ali, Sept70).
vii. Do not use personal information or words in dictionary spelled backwards (such as, AISHAR, ilA, 07tpeS).
viii. Create passwords that can be easily remembered for example taking a first letter of every word in a phrase. (such as, “In The Name Of God For Mankind” and the password could be: "ItNoG4M".

5.1.2 Password Usage

i. Use different passwords for different accounts, systems and applications.
ii. Do not set the "Remember Password" feature of applications or operating system (e.g., OutLook, Netscape Messenger, Windows 2000).
iii. When a password is assigned for a user (either because it is a new user ID or a password had to be reset), the password should be changed the first time that s/he logs on.
iv. If an account or password is suspected to have been compromised, report the incident to system administrator and change all passwords.

5.1.3 Password Protection

i. The recommended change interval for all passwords (e.g., email, web, desktop computer, etc.) is every four months or at least every six months.

ii. Store passwords securely and do not leave it where others can find them. Upon the knowledge that a password has been compromised, do not hesitate to change it to avoid system being invaded by outsiders.
iii. Passwords must not be inserted into email messages or other forms of electronic communication.
iv. Passwords should never be written down or stored on-line.
v. Do not share or reveal a password to anyone.
vi. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Personal Digital Assistant (PDA) or similar devices) without encryption.

5.2 Virus Attack [2]

Virus is a program that can infect another program by modifying the content of a file. It can potentially affect any type of computer or server. The area of greatest risk is personal computers that receive files from external sources, whether over a network, or via shared detachable storage devices. Virus spreads easily when a file is shared amongst users, for example through file transfer and using a diskette. Some viruses attack may corrupt the hard disk and even make it unusable.

There are several types of viruses that include boot sector virus, executable virus, macro virus, Trojans, hoaxes and logic bombs. Viruses, worms, trojans and malicious hackers have long since ceased to be mere irritants, if they ever were that benign. Today they are scourges that demand constant vigilant. If you take no precautions, then sooner or later the data on your computer will probably be stolen or destroyed. Table 1 lists different types of viruses and how they may affect the use of PC.

Anti-virus software is vital to any network security solution. Anti-virus software monitors computers and look for malicious code. The anti-virus software must be installed on all computers for maximum effectiveness. Users must be trained to perform updates for new virus definitions.

The following measures can be taken to reduce risks from virus infections:

i. Ensure that anti-virus software is installed on a PC.
ii. Scan hard disk for viruses once a week.
iii. Update anti-virus definitions once a week. However, if a new virus spreads out, anti-virus definitions should also be updated immediately.
iv. Do not open e-mail attachments from unfamiliar sources or with suspicious content. Delete these attachments immediately, and then empty your Trash to ensure the attachments are no longer exists in the PC.
v. Never download files from unknown or suspicious sources.
vi. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

vii. Always scan a floppy diskette from an unknown source for viruses before using it.
viii. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Table 1: Types of Viruses

Type of Virus	Potential Sources	Means of Infection	Effect
Executable File Virus	i. Infected files/applications download from the network. ii. Infected files shared between users. iii. Infected file attached to mail message. iv. Infected file on purchased software.	Load and execute an infected executable file.	Corrupted file, whole hard disk or consume system resources such as CPU time, memory and hard-disk space
Boot Sector Virus	i. Any formatted diskette. ii. Same as the executable file virus.	Boot from infected floppy	Corrupted hard disk and diskette
Macro Viruses	Same as the executable file virus.	Load infected Word Document or Excel Spreadsheet under MSoft Office Application	
Trojans	i. Same as the executable file viruses. ii. Execute auto-download Trojan applet by Web browser	Run Trojan file	Corrupted file/hard disk
Hoax	E-mail	Chain-letter effect	Slows down the network
Logic Bomb	Same as the executable file viruses.	Coded into custom programs	Corrupted file/hard disk

5.3 E-Mail Security

E-mail is any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of communication across computer network systems between or among individuals or groups. It is a key communication medium by FSKSM staffs.

The most common mail transfer protocols are SMTP, POP3 and IMAP4. These protocols provide basic requirements for e-mail. They do not provide authentication as part of the core protocol, thus allowing e-mail messages to be easily forged. These protocols also do not use encryption to secure the privacy of e-mail messages. However there are extensions for authentication and encryption for these basic protocols. It is recommended to use these extensions in order to secure e-mail messages.

E-mail client can be set to check e-mail automatically at every interval chosen by the user. Every time the e-mail client does the checking, it will transmit user's password to the e-mail server and some systems does not encrypt the password while transmitting it over the network. If the e-mail client does the checking at short intervals, this means that the password will be transmitted across the network many times. Therefore it will be easier for an eavesdropper to capture the password and use it to hack the system.

Some examples of threats when using e-mail are impersonation, eavesdropping and mail-bombing. The e-mail sender can create a false return address and therefore the address on Internet e-mail cannot be trusted. A person can also impersonate by modifying the e-mail header or by connecting directly to the SMTP port on the target machine.

A person can capture e-mail headers and contents during transmission because e-mails are transmitted in the clear format. Therefore, the contents of a message can be read or modified in transit.

Mail-bombing is an e-mail attack whereby the system is flooded with e-mail messages until it fails. The mail is sent to urge others to send massive amounts of e-mail to a single system or person, with the intent to crash the recipient's system. Typical failures are e-mail messages are accepted until the disk where e-mail messages are stored fill up and the incoming queue is filled with messages to be forwarded until the queue limit is reached and therefore no more messages can be accepted.

The following measures can be taken to reduce threats that can occur through e-mail:

i. Choose good passwords for your e-mail account as proposed in 5.2.2.
ii. Do not CONFIGURE e-mail client to automatically check e-mail at every short interval for example for every minute.
iii. When sending an e-mail attachment, make sure that some information about the attachment is mentioned in the e-mail. With this information the sender can ensure that the attachment is legitimate.
iv. Ensure that the installed anti-virus software checks all incoming e-mail attachments.
v. Do not send confidential information or document through e-mail (such as examination questions and results) unless it is encrypted.

vi. Ensure that e-mail received is from the legitimate person to avoid impersonation by intruders. Digital signature can be used to prevent impersonation.
vii. It is recommended that APOP is used for protocol for accessing e-mail because it is more secure than POP since it encrypts passwords.

5.4 PC Intrusion

PC intrusion means an attacker gains an unauthorized control over a computer. This can be done locally or remotely. Whenever a PC is connected to a network, either locally or through Internet, it is vulnerable to remote intrusion. Remote intrusion are much more difficult to detect and may occur without user's knowledge. Usually a user notices it after certain damage has been done to his assets.

PC intrusion tools are within easy reach of anyone who knows how to use the World Wide Web (WWW), just by using any common free search engine. Most of these tools are easy to use. There are several measures that can be used to prevent intrusion. This guideline recommends the following measures:

i. All unneeded network services should be disabled. Usually newly installed operating systems enable all available networking features and therefore allows an attacker to explore the many avenues of attack
ii. Install personal firewall (such as Zone Alarm) or any intrusion detection tool on your PC so that the network traffic that enters and leaves your PC can be guarded. This type of software can detect unauthorized activity and alert the PC owner.
iii. Upgrade all operating systems and applications files frequently, using the security patches provided by the developers to fix coding errors in software as these errors are vulnerable points that often allow pc intrusion by attackers. Recommended duration is once a month.
iv. Encrypt confidential documents before transmitting it across the network or when keeping it in local hard disk.

5.5 Administrative Responsibility

Individual user is responsible for the security of his/her own PC. However the network management is under the jurisdiction of network administrator or IT manager. This guideline recommends the following measures for securing faculty wide network:

i. Assignment of IP segment for students should be different from IP segment for lecturers.
ii. Students should not be allowed to have network access through segments allocated for lecturers.

iii. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
iv. Perform password checking by using password cracking on a periodic or random basis to ensure users use strong passwords. If a password is guessed or cracked during one of these scans, the user will be required to change it.
v. Scan e-mail attachments at the e-mail server so that the majority of viruses are stopped before ever reaching the users.
vi. Install firewall at the server to prevent intrusions. A well-configured firewall will stop the majority of publicly available computer attacks.
vii. Check event logs for any suspicious or abnormal event at the server daily.
viii. Scan a network by using vulnerability scanners to look for computers that are vulnerable to attacks and inform the owner.
ix. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Every network, no matter how secure, has some security events (even if just false alarms). It is recommended that the faculty should form a unit that provides the incident response handling service for the faculty. The incident includes intrusion, denial-of-service, virus, and e-mail abuse. The unit is responsible for identifying how the intrusion occurs, how much damage is done and how to recover, such as broadcasting warnings of any new viruses that appear and how to prevent the attack from these new viruses. This incident response unit will take both prevention and detection techniques of the intrusions. With this unit, any staff who has security problems and does not know how to handle it can refer to the team in this unit.

5.6 General Security Recommendations

This section covers all other security measures that are not mentioned in the above guideline but they are equally necessary. The section is divided into three parts: Good Security Practices, Ethics and Training.

5.6.1 Good Security Practices

i. Never leave a PC running or printers printing unattended while it contains information that should not be seen by others with physical access to it especially while confidential or sensitive information such as examination questions is displayed on the screen.
ii. Log-off or lock PC by using a password-protected screensaver with the automatic activation feature set at 10 minutes or less when the pc is unattended.
iii. Monitor screens, printers, and other devices that produce human-readable output should be placed away from doors and windows. This helps ensure that casual passersby cannot read information from them

iv. Lock the door when leaving a room.
v. Back up important documents regularly and store the backup files in a secure location off site. Recommended duration is every six months.
vi. Do not expose magnetic media from smoke, dust, magnetic fields, and liquids.
vii. Smoke detectors should be installed in the room.
viii. Computers should not be placed under a ceiling which conceal plumbing or other sources of water.
ix. Use original application software provided by the faculty.

5.6.2 Ethics

Staff of FSKSM should abide the following guidelines:

i. Do not reveal any password to others or allowing use of the password by others. This includes close friends or colleagues.
ii. Do not copy someone else academic materials such as lecture notes without informing the owner.
iii. Do not introduce any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
iv. Do not disable faculty network communication without early notification to other users.
v. Do not disrupt faculty network communication for malicious purposes such as network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
vi. Do not log into a server or account without any access authorization.
vii. Do not execute port scanning or security scanning without authorization from network administrator.
viii. Do not use unauthorized or forged email header information.
ix. Do not send or forward "chain letters", or other "pyramid" schemes of any type.
x. Do not use pirated software.
xi. Test all software downloaded from the public domain for errors and malicious logic before it is exposed to operational information.
xii. Use only authorized physical computer resources. Do not provide false or misleading information to gain access to computing resources.

5.6.2 Training

Majority of academic assets are in an electronic form. Some of this information is confidential and therefore it is necessary for every staff in the faculty to be aware of security measures in handling these electronic academic assets. Therefore the faculty management needs to provide training to all staff in order to support faculty's efforts to

maintain secure academic assets. Besides ICT security, the faculty should also provide physical hazard training such as the use of fire extinguishers. Refresher courses should also be done regularly so that the staffs are always sensitive to these security needs.

6.0 Conclusion

The use of ICT in UTM has increased significantly in the past years. In respond to this there is a need for security awareness amongst the staffs since each staff has to manage his/her own PC. Therefore it is necessary to have Guidelines of Electronic Academic Assets that can be followed by the staff. Besides the guideline, the staff should also undergo a security awareness training program so that they can understand the potential threats and the risks that may be encountered when vulnerabilities exist in their PCs. In addition, there should be regular reminders of security threats and solutions by IT administrators.

UTM is in the stage of formulating IT Security Policy. The policy may include hardware/software security, proper physical, procedural, and personnel access controls. The guideline in this document can be used as a starting point in drafting the policy. With the application of security policy in the academic environment, the security of academic assets can be enhanced and the network as a whole can be trusted.