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.

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

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.

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 mailbombing. 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.

Mailbombing 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.

5.6.3 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.