UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Centre of Information
and Communication
Technology (CICT)

POLICY & REGULATIONS

INFORMATION COMMUNICATION TECHNOLOGY (ICT)

UNIVERSITI TEKNOLOGI MALAYSIA

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

DEFINITION

Administration e-mail account E-mail account using **utm.my** domain that is given to person in authority such as deans, deputy registrar. (example: fsksmdean@utm.my).

Application Program developed to execute certain specific task such as Financial Information System, Academic Information System and the like.

Attachment Any electronic file attached to an e-mail

Audit Trail Refers to a chronological sequence record audit, each containing direct evidence about and also resulted from implementation of a business process or system function

Availability Measure of an equipment or system whether operating according to functional specification.

Back up Data Replicated data such that the data can be used for recovery in the event of a disaster.

Bandwidth Rate of data transfer in an electronic communication system.

Bomb e-mail Repeated transmitted mail causing the inbox of recipient to be full and not able to function properly.

Borrowing of ICT Equipment The process of giving and supplying ICT equipment within the period specified through a valid application process.

Broadcasting Whatever means that enables digital data and information to be shared and accessed by other users using electronic media.

Chat Room Chatting in the cyber space within a group for specific topic.

Commercial Transaction A financial transaction that involves a change in the financial status of two or more individual or business.

Communication Exchange of information and data between individuals and group through electronic media.

Computer Lab Facility provided by the university to support activities related to administration, learning, development, research and services. Computer lab usage encompass activities carried out in the lab (in person) or through on-line access to the

DEFINITION

lab.

Cracked games Pirated commercial software shared with the consent of the owner.

Domain Registered named used in a network computer system.

Gator Company known as Clara *Corporation* which provides application with advertisement according to the user's habit.

Group e-mail account E-mail account using **utm.my** domain that refers to a special group account. (example:rmc.rnd.net@groups.utm.my).

Hardware Equipment and ICT component such as computer, notebook, printer and the like.

Hot bar & Search bar Program which resides at the top of an Internet Explorer browser. This program monitors information about the web page visited and keeps a history of data searched using search engines.

ICT Information and Communication Technology.

ICT Facility Including but not limited to personal computer, computer peripheral, computer communication, computer software, manuals, storage equipment, support facilities and human resource. Facilities is limited to facilities purchased, rent, leased or lent to the university.

Incidence An event or situation causing interference to ICT services.

Individual e-mail account Individual e-mail account that uses **utm.my** domain (example: aziz@utm.my).

Internet Accessibility Refers to access quality of an Internet service as to whether it is accessible, slow or fast.

IP (Internet Protocol) Internet Protocol (IP) refers to protocol used for data communication across internet network using Internet Protocol Suite. IP number refers to a unique number assigned to a communication device (e.g. a computer).

Junk or spam mail Similar e-mails sent from an unknown or uninvited user which normally carries elements of advertisement

DEFINITION

List Internet user directory stored for the purpose of communication.

Main page Refers to front page of the university web page.

Malicious code Program such as virus, worm and Trojan running illegal process on a computer or computer network.

Malware & Malicious Codes Abbreviation for *malicious software*, i.e. software or a piece of code designed to disrupt operation of a computer system. *Trojan, spyware, adware, worm* are examples of *malware*.

Metadata Information about web site page contained at the start of the web site program.

Moderator A member of a group mail account responsible to manage the group mail.

Network Equipment Equipment and component used in a network system such as a switch, hub, router and the like.

Peak Load Time Time and period when access to the internet are high. Currently the peak load time at the university is between 8.00 am to 5.00 pm.

Signature A feature available on an e-mail service that allows user to write their name and address on every mail sent.

Social network A network amongst a group who interacts amongst themselves and influences each other. This network happens through a system like Friendster and the like.

Software Computer program used to execute specific task such as office automation software, graphics software and the like.

Spyware & Adware Software to gather information about users connected to the internet without the knowledge of the user. Normally this is used for the purpose of advertising using pop-up message.

Staff A person appointed by the university for a permanent, part time, temporary or contract position and still servicing the university.

Storage Data storage or information in any file format (text, voice, photo, movie, software etc) for the purpose of digital

DEFINITION

recovery and sharing.

Student A person who registered and having an active status for an academic program (whether full or part time or postgraduate) in the university .

Thumb drive A form of external storage that exhibits the characteristics of hard disk and connected to the computer via a USB connection.

Trojan ***Malware*** are program which are seemingly harmless but quietly can bring damage to the computer.

University Web Page Covers the University / Faculty / Centre/ Department / Unit / Organization web site (except individual) placed under the **utm.my** domain or any domain recognized by the committee elected by the university.

University Web Page Administrator Refers to an officer officially appointed by the university or faculty or department to administer a web site.

URL **Universal Resource Locator** – is an introduction or marker to access certain website location

Users A person or group of people allowed to use the university ICT service.

UTM Disclaimer Statement which denies any responsibility and rejects any claims by an individual or external organization to UTM on an issue, an example is the outcome after using UTM e-mail system.

UTM e-mail administrator A CICT staff or a staff appointed by a faculty or unit assigned to administer the e-mail system.

Virus Program or code inserted in a computer without the knowledge of the computer owner and executing computer operations without the knowledge of the computer owner.

Web page A location in a *World Wide Web.* Every web page contains a main page i.e. the first page displayed to users when a visitor visits a web site.

DEFINITION

Worm	Program that has the ability to replicate itself in a computer system and has the ability to congest the network traffic, increasing operating load and the like.

A. INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

1 INTRODUCTION

The ICT services in UTM is aimed at helping the university achieve its vision and mission in tandem with the aim of promoting development and success in the country as well as for the benefit of mankind. In the effort to achieve this, the university is providing ICT services for the campus's community to be used to improve the quality of teaching and learning, research activities, consultancy as well as the administration of the university.

The ICT policy is implemented for use among the people in UTM to ensure a systematic use of the ICT which is in accordance with the guidelines.

The eight ICT procedures of the policy are as follows:

1.1 Procedures for Internet Use

1.2 Procedures for E-mail Use

1.3 Procedures for Contents and Publications in the Website

1.4 Procedures for Distribution and Use of Computer Hardware among Staff

1.5 Procedures for Use of Computer Labs

1.6 Procedures for Loan of ICT Equipment

1.7 Procedures for Disposal of ICT Equipment

1.8 Procedures for ICT Security

2 OBJECTIVE

The aim of the ICT policy is to provide procedures on the use of ICT in the university. The policy is meant to safeguard the university from any legal implications as well as educate the campus's community to have social awareness and intellectual responsibilities on the use of ICT. The policy is also to ensure availability, integrity and confidentiality of ICT services in UTM are achieved.

3 SCOPE

The UTM ICT services will be given to every member of the campus's community who is eligible and registered with the university. The services would also be provided to guests permitted by the university

4 METHODS OF ICT USE

The campus's community can have access to the services provided by ICT by using different access methods approved by the university.

5 IMPLEMENTATION

The policy on the use of Internet and e-mails was developed in 2008 which was improved further before it was presented for approval in order to be implemented in June 2009.

6 LOCATIONS OF ICT SERVICES

The campus's community can use the ICT services available at the faculty, office, colleges as well as other locations determined by the university

7 OWNERSHIP

Any electronic file that is produced, printed, sent, received and stored in the computer owned, rented or managed under the administration of UTM will belong to UTM. However, the ownership does not include the intellect property of the original owner.

8 PRIVATE OWNERSHIP

The use and applications of systems from ICT used by the individual such as e-mails, blogs, electronic files and other social network systems such as MySpace, Facebook, YouTube, etc that are downloaded; stored and accepted in the computer system will not be owned by the individual. Any information can be accessed if it is meant for administration and maintenance of information system, solving technical problems, security management system, and management review, following a court order, internal audit system or other audit system and related policies.

9 INCIDENTAL USE

9.1 Personal internet access from within or outside the university is limited to registered users only. The access does not include use by family member or other parties.

9.2 Incidental use should not increase the additional cost to the university.

9.3 Incidental use should not affect the quality and performance of the user.

9.4 Ensure that files or documents sent or received will not have legal implications and tarnish the image and reputation of the university

9.5 Storing of electronic files and documents kept in the ICT system must be kept minimal.

9.6 Any files or documents inclusive of official personal documents of users belong to UTM and can be accessed at the discretion of the university or in accordance with its regulations.

10 DISCIPLINARY ACTIONS

Any act against the policy will result in disciplinary action taken on the student or staff. The person can be prevented from using the ICT services. Students who go against this policy will face disciplinary actions in accordance with Universiti Teknologi Malaysia Procedures (Students Discipline 1999). Permanent staff of the university will face disciplinary actions under the Act of Semi-Government Agencies (Discipline and Surcharge) 200 (Act 605) or any relevant Acts.

a. Constitution of Universiti Teknologi Malaysia -S6 (1)(r)
b. Secret Official Act 1972 – disseminating official secrets illegally m - S8
c. Communication and Multimedia Acts 1998
d. Computer Crimes Act 1997
e. Changes without authorization– S5
f. Miscommunication – S6
g. Accomplice and Attempts– S7
h. Telemedicine Acts
i. Digital Signature Act 1997

Contract, temporary or part-time staff may also face appropriate disciplinary actions including termination of service.

B. PROCEDURES ON THE USE OF INTERNET

1 INTRODUCTION

Internet is a global network communication system that allows anyone to share information and interact with others. The Internet service provided by the university is used by students and staff in their daily activities as a means of communication with others. This electronic communication is a very important channel for sharing knowledge. By having guidelines for Internet use, the risk of Internet disruptions in the university can be reduced.

The guidelines adopted and adapted in this policy are based on the **Public Services Development Circular 1 2003; Guidelines for Appropriate Use of Internet and Electronic Mails in Government Agencies.**

2 OBJECTIVES OF PROCEDURE

The objectives of the procedure are as follows:

2.1 Support and implement the vision and mission of the university

2.2 Describe usage procedures for the Internet provided by the university

2.3 Increase the security of official documents within the Internet environment.

2.4 Ensure a systematic and control of Internet use amongst the users in the university

2.5 Decrease risk of operational disruptions to the Internet

3 SCOPE OF PROCEDURE

The guidelines will cover Internet Use provided by the university.

4 PROCEDURE STATEMENT

4.1 The use of the Internet is meant to support the core mission of the university in teaching, learning, research and consultancy

4.2 Internet use for the applications listed previously must acknowledge ownership, intellectual property and rights of individual users.

4.3 Internet use by people in the university is a privilege and not an absolute right of use

4.4 Academic and administration Internet use will be given priority during peak hours as compared to the users in the university colleges.

4.5 Internet users are responsible for the integrity and security of the identification details (ID) and password to access the network and other systems in the university.

4.6 Internet Use by the users in the university should not disrupt access and affect the ability of the IT infrastructure. Downloading large data which may monopolize the bandwidth using P2P or similar protocols is considered disrupting access and reliability of the services.

4.7 The university has the right to ensure that online applications utilizing high resources such as video streaming do not disrupt the accessibility and reliability of ICT infrastructure.

4.8 Users are responsible for information disseminated by checking the validity of the information or obtaining prior consent from the owner.

4.9 Users are responsible for ensuring that the devices accessing the internet are free from malware such as *spyware, adware* and *virus.*

4.10 Internet commercial transactions are not allowed. If a user has been found to have done such a transaction for personal use, the university can take appropriate actions and the university is not responsible for any loss or damages incurred by the user.

4.11 A user who uses a service that requires payment in electronic business transaction such as use of credit card, PayPal, online banking, etc. is responsible for all his online transactions.

4.12 A user must inform Centre for Information and Communication Technology (CICT) if he suspects or knows of a situation that might jeopardize the security of the communication in the university.

4.13 Dissemination of pornographic, lewd, malicious, threatening and political materials are prohibited.

4.14 The university has the right to revoke the privilege of Internet Use if there is any abuse of the rules and policy prescribed by the university.

4.15 The university may refer to the appropriate authorities for advice on the actions to be taken to ensure that going against the rules and policy will not be repeated.

5 GUIDELINES

5.1 Refer to the University Teaching and Learning Policy 2007 on activities for teaching and learning.

5.2 Refer to the University Policy on Research 2008 for research activities

5.3 Refer to the University Policy on Consultancy 2008 for consultancy activities.

5.4 Users should use the password for screen savers and logging off of the computer

5.5 *Chatting, forum*, *Instant Messenger* and the related technology using Internet used for communication are limited to its use for teaching, learning, research, management and administration.

5.6 To ensure availability of bandwidth for every user in the university, the university has the right to limit and set the appropriate maximum amount of data that can be uploaded and downloaded from time to time.

5.7 Data storage provided by the university is limited to its use for purposes such as teaching, learning, research, publication, writing, consultancy and related supporting activities.

5.8 Dissemination, storage, downloading and uploading of pornographic, lewd, malicious, threatening, business and political materials are strictly prohibited.

5.9 Refer to University Policy of Intellectual Property 1999 for Copyright and Intellectual Property issues.

5.10 Activities such as hacking, scanning, sniffing, phishing and decrypting of data illegally from inside and outside of the university is against the act of privacy and not allowed.

5.11 The Internet user responsible for uploading and disseminating information should check for the validity and the most updated version as well as obtain permission for using the information meant for dissemination.

5.12 Users must abide by the University ICT Security Procedure when using and managing their IDs and passwords.

5.13 Users are responsible for using original operating system and applications and updating them. The university is not responsible for any legal implications for use of pirated software.

5.14 Users are responsible for installing anti-malware (anti-virus, anti-spam, anti-spyware, anti-adware) and should update them for the device used.

5.15 Users are responsible for scanning the system in the device using anti-malware software at least once a day.

5.16 Users are advised to keep the device in an area that is physically safe from unauthorized users or any illegal access

5.17 Users are not permitted to install software for purpose of gambling, games, hot bar, search bar, gator or surfing prohibited websites such as cracked games, online games or hacking other computers owned by the university.

5.18 Any form of commercial advertisements offered by the search engines such as Google Adsense is strictly prohibited.

C. PROCEDURES FOR E-MAIL USE

1 INTRODUCTION

E-mail is a service provided by the internet that is widely used nowadays. The e-mail application is used extensively and allows different types of communication to take place at a very fast rate. Its application is suitable for brief forms of writing. Every student and staff in the university is given an e-mail address and should use it actively.

The guidelines adopted and adapted by the university are based on the Public Services Development Circular 1 2003; **Guidelines on the Appropriate Use of Internet and Electronic Mails in Government Agencies (Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-Agensi Kerajaan).**

2 OBJECTIVES OF PROCEDURE

The objectives of the procedures are as follows:

2.1 Explain the rules and ethics of using the university's e-mail

2.2 Outline the ethics and safe use of e-mail order for the service to be beneficial for staff and students..

2.3 Reduce risk of disruptions of internet and e-mail operations.

3 SCOPE OF PROCEDURE

The guidelines apply to staff, students and those who are permitted to use the university e-mail such as Siswa Mail, Webmail UTM, faculty e-mail, etc. The guidelines consist of

3.1 Individual e-mail account

3.2 Administration e-mail account and

3.3 Group e-mail account.

4 PROCEDURE STATEMENT

4.1 All university e-mail accounts are owned by the university

4.2 Official duties conducted on the internet must use the offical university e-mail and its use must be standardized in accordance with the provided offical rules.

4.3 Users are not allowed to abuse the e-mail application such as to incite and defame others, send false news, retransmit copyrights or activities prohibited by cyber law.

4.4 Official e-mails that are restricted, confidential, secret or top secret must be protected for the sake of security.

4.5 Use of inappropriate and excessive language in official e-mails are strictly prohibited.

4.6 Users of university e-mail accounts are responsible for the contents, management of the storage and security of their e-mails

4.7 Every university e-mail must have the university Disclaimer and the official signature of the e-mail user at the end of the email.

4.8 Users should not allow a third party acting on his behalf to reply to the e-mails sent to the user

4.9 The university e-mail accounts may be revoked at any time in cases when there are inappropriate actions against the rules for using university e-mails.

4.10 Group e-mail account must be officially formed at university level and managed by a moderator.

5 GUIDELINES ON E-MAILS USAGE

5.1 Use of university e-mails are strictly prohibited for the following:

5.1.1 Activites against the laws of the country.

5.1.2 Duties that are in not accordance with the government's principles and regulations.

5.1.3 Commercial purposes which have no relevance to the university.

5.1.4 Personal business activities.

5.2 E-mail users must ensure that the contents of the e-mails do not contain confidential information which might be used to tarnish the reputation of an individual, organisation or country.

5.3 Users are encouraged to use protocol facilities such as https to send their e-mails in a safe and secured environment.

5.4 Users are advised against writing personal or confidential matters in their e-mails. If there is a need to do so, users should take the necessary steps to ensure security by using e-mail encryption facility.

5.5 Users must keep their passwords to themselves and not tell others about them.

5.6 Users must be cautious when using university e-mail through public computers to ensure that the computer does not save the ID and password information of the user. User must ensure he is to logged out upon terminating the mail application.

5.7 Users must contact the e-mail administrator immediately if they detect or suspect that the university e-mail account is being compromised by a person or in cases of impersonating university e-mail account.

5.8 Users are responsible for informing the university e-mail administrator if they will be working outstation for long periods of time, on leave or transfer to another place of work to facilitate maintenance..

5.9 Users must limit the number of e-mails in their e-mail boxes according to the storage space given by the university e-mail administrator. Irrelevant e-mails should be deleted.

5.10 Users are responsible for copying and duplicating the digitized data and save them into a second storage facility such as diskette, etc for security reasons.

5.11 Users can request for a University Disclaimer from the university e-mail administrator.

6 PREPARING AND EDITING MAILS

6.1 Users are encouraged to write about a single topic only in one e-mail.

6.2 Users must ensure that the subject and contents of the e-mail are similar. The title of the e-mail will inform the receiver of the importance of the e-mail.

6.3 Users are encouraged to write e-mails using the formats of writing documents. The contents of an e-mail written in capital letters is an indication of a warning message.

6.4 Users are encouraged to use attachment in their e-mail if a file with the information is already available such as minutes of a meeting that is saved in the Microsoft Word.

6.5 Users must ensure that the attached files are free from virus.

6.6 Users must ensure that the size of the attached files is not more than the maximum allowable size. If the file is too big, split the file into several small files and send the files separately or zip the file.

7 SENDING E-MAILS

7.1 Users must be cautious about sending e-mail as it is difficult to retract once it is sent.

7.2 Ensure that the e-mail contents is complete and conveys the intended message.

7.3 Check that the email address is correct. An e-mail address may be used by an individual or a group.

7.4 Users are encouraged to respond to their e-mails within four days of receiving the e-mail.

7.5 Users are reminded not to be involved in sending junk mail or bombarding e-mails.

7.6 Users are advised to use the facility appropriately;

7.6.1 cc (carbon copy) – a copy of the e-mail to be sent to another person

7.6.2 bcc (hidden copy) – a copy of the e-mail sent to another person without informing the other mail recipients. Users are advised not to use this facility due to transparency issues.

7.6.3 reply– response to an e-mail received from a sender

7.6.4 all –response to an e-mail from a sender that will also be sent to other recipients who are in the cc list.

7.6.5 forward – sending the received e-mail to other recipients without editing the original contents of e-mail.

8 TO BE A MEMBER OF A GROUP E-MAIL ACCOUNT

8.1 Users can join any university group e-mail account if it is appropriate for their position in the university such as academic group e-mail account, Example is academic network for professional discussion.

8.2 Users are advised to be careful if they are registering with a group e-mail account as this might cause their e-mail box to be full if the account is not managed properly. Contact the moderator of the account if you would like to withdraw your e-mail account from the group.

8.3 Users who have registered in a group e-mail account should be an observer for the first few days. Watch and observe the nature of the discussions. If the user is satisfied with the discussions, then he may take part in the discussion.

8.4 Users are advised to be honest and ethical with their answers if a person requests a service or advice. Personal e-mail comments should be sent to the recipient only and not sent or copied to an e-mail mailing list or discussion group.

8.5 Users are reminded that every member in the discussion group is entitled to their own opinion and has their own expertise, preference and stand. Please use references to explain complicated or unacceptable issues.

8.6 Users are advised to question or comment within their group only. If there are members who have created problems by sending inappropriate information, then the user should respond politely and avoid any arguments.

D. PROCEDURES FOR CONTENTS AND PUBLICATION IN WEBSITE

1 INTRODUCTION

The contents of the university website are very important to present and disseminate the latest information and activities to the society in campus as well as other users. The correct organization of the contents in the website will ensure that the information is useful and effectively presented. The contents and layout of the website are the responsibility of the appointed university website administrators

The guidelines adopted and adapted are based on the **Public Circular No. 1 Year 2006, Website Management/Public Services Sector (Pengurusan Laman Web/Portal Sektor Awam)**

2 OBJECTIVE OF PROCEDURE

The aims of the procedures are as follows:

2.1 Guide the administrators of UTM websites such as University/Faculty/Center/Department/Unit/ Association or to whom it may concern about completion of contents suitable for UTM websites

2.2 Ensure that the information and materials in the websites are standardized, controlled, secured and in accordance with the requirements of the university management.

2.3 As a reference for developing and managing the university website.

3 SCOPE OF PROCEDURE

The procedure are used for the following:

3.1 Apply to information and materials which will be or has been inserted in the university website

3.2 Every website under the domain utm.my under the supervision of the University /Faculty/ Center/ Department/Unit/ Association and managed by the appointed university website administrator.

3.3 Administrators of the university websites and responsible parties for managing and inserting the contents of the websites belonging to the university.

3.4 The university has the right not to publish web sites that does not conform to the procedures and specifications stipulated.

4 PROCEDURE STATEMENTS

4.1 CONTENTS OF UTM WEBSITE

4.1.1 Contents of UTM website is determined by the respective units but is governed by the regulations and instructions given by the university form time to time.

4.1.2 Contents in the university website must be approved by the authorities responsible for managing the university website.

4.1.3 Contents placed in the university website is governed by the rules and Acts of copyright, intellect property and Trademark.

4.1.4 Contents in the university website should not contain any form of materials that are against the law of the university, state and country.

4.1.5 The administrator of the university website has the right to change/adapt/delete contents that are not suitable for the sake of security and effective use.

4.1.6 The administrator of the university website is responsible for ensuring that the information in the website is updated accordingly.

4.1.7 The administrator of the university website is responsible for the contents and security of the website.

4.1.8 Individual website using the *utm.my* domain is the responsibility of the individual but is governed by these guidelines

4.1.9 The language used in the main page of the website is in accordance with the current rule adopted by the university. However, the facility to choose other languages must be placed on the front page.

4.2 DESIGN OF THE WEBSITE

4.2.1 Design of the main page in the University/Faculty/Center/Department/Unit/ Association website must be inline with theme and standard determined by the university.

4.2.2 The design must be user friendly, attractive and easily accessible.

4.2.3 The structure of the contents in the main page of the website must follow the format given by the university. However, the expansion of the structure is allowed depending on the function and needs of the respective unit.

4.2.4 The organization of contents or elements in the website must be standardized and consistent for every page in the same website.

4.3 LANGUAGE VERSIONS

4.3.1 Every website must have the version in at least two languages which are Bahasa Melayu and English.

4.4 INTERACTION FACILITIES/HYPERLINKING AND SEARCH

4.4.1 Every website unit must have a hyperlink to the university main website.

4.4.2 Links to websites that are out of the main university website is governed by the university regulations and related Acts.

4.4.3 Every unit must provide a search engine or an effective information search facility for users.

4.5 WEBSITE SPECIFICATIONS

4.5.1 Specifications of Website

4.5.1.1 Every website must have features that represent the unit or contents that reflect the website.

4.5.2 Use of Logo

4.5.2.1 Every webpage in the official website must have the official university logo.

4.5.2.2 The position of the logo must be placed consistently and at the same position in all the web pages.

4.5.3 Typographical Aspects

4.5.3.1 Selection of typographical aspects should take into account the clarity and comfort of the readers.

4.5.3.2 The typographical aspects should also take into consideration printing requirements.

4.5.4 Use of Multimedia Elements (Graphics, Animation, Audio and Video)

4.5.4.1 Use of visuals such as photographs, graphics, animation, video clip, etc must be suitable in terms of size, accessibility and user friendly.

4.5.4.2 Downloading of photographs can only be done with oral or written approval by the owner for record purposes or if it involves official university activity.

4.5.4.3 Any use of audio visual elements in the website are under the Acts of Copyright, Intellect Property and Trademark and approval from the original rightful owners must be obtained before they are used.

4.5.4.4 Downloads of multimedia elements into the university website must not have any feature that is against the laws of the university, state and country.

4.5.4.5 The multimedia elements in the university website should not exhibit any feature that might offend an individual, society, religion or race.

4.6 DOMAIN NAMES AND URL

4.6.1 This policy explains the framework for architecture and UTM's information infrastructure based on web so that ascertainable effective information can be achieved to the targeted users. All university entities are required to publish their web content with the name utm.my. This naming can contribute the university's web ranking.

Entity	URL Names
Faculties, SPS, CTL, RMC, BIP, PSZ, SPACE, Centre of Excellence and *Research Alliances*	www.*entity*.utm.my example: www.fka.utm.my www.centre-of-excellence.utm.my www.cepp.utm.my
Departments under faculty	www.utm.my/faculty example: www.fsksm.utm.my/software-engineering
Office / Strategic Units in UTM	www.utm.my/office example: www.utm.my/corporate-affairs
Official Staff Organization / Clubs	www.utm.my/name-of-club example.: www.utm.my/wangi
Official Student Organization / Residential Colleges / Club	www.utm.my/name-of-club example: www.utm.my/utm-netball-club example: www.utm.my/kolej-rahman-putra
Events	www.utm.my/event example: www.utm.my/citra-karisma

4.6.2 Use lower case for all URL's

4.6.3 Underscore are not to be used in the URL, instead hyphens are to used,

Example:
www.utm.my/staff-info and not www.utm.my/staff_info

4.6.4 Do not combine two words to be one when naming URL

Example:
www.utm.my/corporate-affairs and not
www.utm.my/corporateaffairs

4.6.5 College, Departments and other units in the university must name their domain that represents the university or the university's service.

4.7 ADVERTISEMENT

4.7.1 Third party advertising or commercial promotion of group not from UTM / organization / individual are not allowed on any of the university network or university web page.

4.7.2 All official advertising websites official must follow the copyright materials policy.

4.7.3 Any sales of pornographic materials are not allowed in any of the advertisement within the university web page.

4.8 WEB ACCESSIBILITY

4.8.1 University's web site must be accessible and readable to all categories of users including disabled people. Web accessibility is vital so that all the information related to teaching and learning can be accessed by all.

5 GUIDELINES

The purpose of this guideline is to assist designers, developers and content editors from all level of competency to create, maintain and manage high quality web sites

5.1 CONTENTS OF WEBSITE

5.1.1 Contents of the university website should take into consideration the main aspects underlying the rationale for setting up the website specifically meant for disseminating information needed by the targeted group.

5.1.2 Use of contents involving Copyright, Intellect Property and Trademark must have permission from the owners before they are inserted in the university website.

5.1.3 Every unit must have a structure and consent procedure for every content and adaptations to be made in the respective unit's website.

5.1.4 The contents of a current website must be updated within a reasonable time frame or time given. The date of the update must be presented at the bottom left side of the main webpage.

5.1.5 Every unit must have a mechanism that is suitable and effective for providing security for the contents of the website from being hacked or tampered by irresponsible parties.

5.1.6 Every unit must ensure that the contents of the main page in the website must have the following:

5.1.6.1 Texts or graphics that contain the full name of the respective unit.

5.1.6.2 Staff Directory

5.1.6.3 Communication Information – address/ telephone number/ fax/ e-mail

5.1.6.4 Information For & Information About

However, each unit may include more information related to the functions and needs of the unit as follows:

5.1.7 Introduction/ Welcoming Speech

5.1.8 News or events

5.1.9 Main News or Current News

5.1.10 Upcoming Events

5.1.11 Organization – Organizational Chart

5.1.12 Academic – Academic Information

5.1.13 Research – Information about research, research grants, research expertise, publication and accomplishments.

5.1.14 Facilities – Research, library, etc.

5.1.15 Hyperlinking – Describe links to the university website and related ones only

5.1.16 Feedback- Responses from the website visitors.

5.1.17 Any additions to the menu are encouraged.

5.1.18 Every main website must have a counter to calculate the number of hits to the webpage.

5.2 DESIGN OF WEBSITES

5.2.1 Every unit must refer to the unit appointed by the university to standardize the theme and concept of the website design.

5.2.2 Design of websites must be user friendly, attractive and accessible.

5.2.3 To ensure that the design is user friendly, attractive and accessible, every unit must consider the following:

5.2.4 Downloading time should be fast and realistic

5.2.5 Use of technology that is suitable and accessible by a majority of the users.

5.2.6 Have an alternative access by providing information in text only mode.

5.2.7 Design a navigation system that is consistent and easy to use for every web page.

5.3 INTERACTION FACILITY/ HYPELINKING AND SEARCH

5.3.1 Every web page has to have the logo or text "Universiti Teknologi Malaysia" that is linked to the main university website.

5.3.2 Every web page must exhibit the copyright notice such as Copyright owned by Universiti Teknologi Malaysia at the very least in the main page

5.3.3 Every web page must have a Disclaimer notice for every external link listed in the university website.

5.3.4 Every unit must ensure that the external links out of UTM website are suitable for use and is important for the university. Any links that may effect the university negatively such as the following list should be avoided.

5.3.4.1 Political Websites

5.3.4.2 Advertising/Business Websites (unless approved by the university)

5.3.4.3 Immoral Websites that are against the ethics.

5.3.4.4 Websites that that may offend the sensitivity of an individual, religion and race.

5.3.4.5 Every university website must provide an application for ease of information search for its users.

5.4 WEBSITE SPECIFICATIONS

5.4.1 The features that would identify and reflect the unit and/or contents of the website should be placed at the Page Title section.

5.4.2 The university logo must be placed on the main page where it is easily seen which is either in the top left or right of the screen.

5.4.3 To improve its application and comfort for the users, the text should have the following features:

5.4.3.1 Use contrasting colours which are against the background for the website.

5.4.3.2 Break a long piece of text into several short paragraphs

5.4.4 Choice of font and size should be based on the following:

5.4.4.1 Taken form the standard collection

5.4.4.2 Use the typing feature from the sans serif category such as arial, tahoma dan verdana, etc. for easy online reading.

5.4.4.3 Do not use too many different types of typing features in the same website.

All elements mentioned below must be available on the developed web site

5.5 OPTIMUM SEARCHING ENGINE

5.5.1 Keywords and Phrase

5.5.1.1 Focus on targeted user's need.

5.5.1.2 There are a number of search engines giving more focus on words and phrases near to the top portion of the displayed page. Thus place the keywords and phrases especially between the title and the first few paragraphs.

5.6 BROWSERS

All developed web site must support at least less Mozilla Firefox and Internet Explorer.

E. PROCEDURES FOR DISTRIBUTION OF COMPUTER AMONG STAFF

1 INTRODUCTION

The extensive use and distribution of computers to eligible users in Universiti Teknologi Malaysia (UTM) has helped improved productivity among staff in their daily duties. This is in tandem with UTM's aspirations of becoming a world class university.

2 OBJECTIVES OF PROCEDURE

The procedure will have details and explanation about managing computer distribution for staff. The centralized acquisition of a computer and its accessories will be the responsibility of the ICT Center. Besides that, the procedure is used to coordinate and standardize distribution of computers in the university.

3 SCOPE OF PROCEDURE

The scope of procedure encompass

3.1 University officially owned hardware and software used or kept by the user without any discrimination of its use.

3.2 Applications developed and owned by the university without any discrimination of its use.

3.3 University staffs that are eligible are as follows:

3.3.1 Special positions such as Vice-Chancellor / Deputy Vice-Chancellor / Registrar / Chief Librarian / Director of Works / Legal Officer / Dean / Deputy Dean / Director / Head of Department / Hostel Warden.

3.3.2 Academic Positions such permanent, contract, department appointed lecturers.

3.3.3 Non-Academic Positions or Administrative or Professional officers (Permanent/ Contract/ Department Appointed) and Administrative staff (Permanent/ Contract/ Department Appointed) who are directly involved with duties that require the use of a PC or notebook and with the approval of the head of department.

3.4 Loan of PC and notebook can be considered in certain cases for the following university staff

3.4.1 Adjunct Professor

3.4.2 Visiting Lecturers

3.4.3 Trainers/ UTM SLAB Candidates

3.4.4 Other Administrative Staff

3.5 The administrative officer in the department (PTJ) is responsible for the acquisition of computers used in Computer Labs for Teaching and Research and has to inform the ICT Center about the acquisition for university inventory.

4 DISTRIBUTION OF COMPUTERS TO STAFF

The procedures are as follows:

4.1 Distribution of hardware must be according to the university procedure.

4.2 Each Academic and Management and Professional Staff will be given a PC or a notebook. Hardware used from other sources will have to be approved by the Chief PTJ. The allocation is based on the seniority of position, job responsibilities and availability of the hardware.

4.3 Staff in other categories is eligible for a PC or notebook based on the requirements of the duties determined by the Chief PTJ.

4.4 Staff who have resigned or retired will have to return the hardware to the PTJ within a week from the effective date or before its due date. The hardware must be returned in a good condition. The ICT Center must be informed of the return of the PC or notebook.

4.5 Replacement of a PC or notebook can be considered after it has been used for three years. However, the time given may change due to technical problems. The final decision lies with the Director for ICT.

5 RE-DISTRIBUTION OF COMPUTERS TO STAFF

The Chief PTJ or authorized officers can do the following:

5.1 Re-distribute the computers formerly given to staff who have completed their services such as contract, retire, termination of service, loss of ability due to health conditions (certified by the Medical Board) to other staff who are resuming the duties of these people or in accordance with the needs of the PTJ.

F. PROCEDURES ON THE USE OF COMPUTER LABS

1 INTRODUCTION

Computer labs are made available by the university to support administrative, educational, developmental and research activities in the university.

2 OBJECTIVES OF PROCEDURE

The procedure on the use of computer labs ensures that:

2.1 The facilities in the computer labs such as the equipment and software are not misused.

2.2 Enforcement of computer labs usage is clarified.

2.3 A suitable environment for computer lab usage is created.

2.4 A sense of responsibility amongst lab users is cultivated.

3 SCOPE OF PROCEDURE

The procedure covers all staff members, students and individuals using the computer labs. The procedure does not cover the management of these labs.

4 LAB OPENING HOURS

The opening hours for computer labs must be specified and users must be notified. * Governed by changes and notice of change.

5 COMPUTER LAB BOOKING

5.1 All lab bookings must be recorded.

5.2 Lab booking must be made according to the specified procedures.

6 REGULATION BEFORE ENTERING A COMPUTER LAB:

6.1 A user must register with the responsible party.

6.2 A user must show his student card or identity card before entering the lab (unless he obtains permission from the lab assistant in charge).

7 REGULATION WHILE IN THE COMPUTER LAB:

7.1 A user must adhere to the account security guideline.

7.2 The user is responsible for his data.

7.3 A user cannot change, move and remove any equipment in the computer lab.

7.4 All forms of computer games are prohibited.

7.5 Users cannot make changes, add or erase any software in the computer system in the lab.

7.6 Users are not allowed to copy licensed software or copyright application from the computer system in the lab.

7.7 Users are not allowed to change the computer program or configure the computer.

7.8 The internet usage in the lab is governed by the guideline of internet use.

7.9 The code of conduct whilst in the computer labs are governed by the university etiquette.

7.10 The user is responsible for the safety of his/her personal belongings.

7.11 The use of private computers in the lab is governed by the guideline on computer usage.

7.12 The use of online facilities in the computer lab is governed by the guideline on computer usage.

8 DRESS CODE

The dress code in the computer lab is governed by the university dress code.

9 COMPUTER LAB CLEANLINESS

9.1 Food or drink are not allowed in the lab (except with permission).

9.2 Littering is not allowed.

10 COMPLIANCE TO RULES DURING EMERGENCY

Should any emergency occur (example fire outbreak or the like) in laboratory, the user must abide security rules available in that laboratory

11 GUIDELINES TO USAGE TIME

Lab booking are to be done or with the authorization of the officer responsible to avoid confusion on the date, time and purpose

12 COMPUTER LAB BOOKING

Lab Booking should be made or authorized by the officer in charge to avoid confusion with regard to the date, time and reason for booking.

13 USE OF COMPUTER LAB

13.1 Phone calls made in the computer lab must be carried out discretely.

13.2 Any problems faced should be referred to the lab assistant on duty.

14 COMPUTER LAB CLEANLINESS

Users are also responsible for maintaining the cleanliness of the lab.

G. PROCEDURES FOR ICT EQUIPMENT LOAN

1 INTRODUCTION

Procedure on the loan of ICT equipment should be adhered to when allowing an individual to loan any university owned equipment.

2 OBJECTIVES OF PROCEDURE

The procedure ensures that users are aware of the etiquette and responsibility related to the loan of university owned ICT equipment.

3 SCOPE OF PROCEDURE

The procedure includes all university owned ICT equipment loaned to users regardless of their location (refer to the guideline on the transportation of assets outside university campus). The users here refer to university staff and students that borrow university owned ICT equipment.

4 PROCEDURE STATEMENTS

4.1 THE USE OF ICT EQUIPMENT ON LOAN

The following are etiquette for the use ICT equipment:

4.1.1 Users are not allowed to handle ICT equipment not under their responsibility. This includes unauthorized using and taking, stealing ICT equipment or components and trespassing ICT labs.

4.1.2 In case of equipment malfunction or breakdown, a user must immediately report it to the responsible party for the purposes of repair.

4.1.3 In case of missing or stolen ICT equipment, a user must immediately lodge a report to the responsible party according to university procedure.

4.1.4 Leaving a computer switched on overnight without reason that is accepted by the university authority is prohibited. Please ensure that electrical switches are turned off before leaving the room or after office hours.

4.1.5 Do not use faulty or damaged electrical cables.

4.1.6 The use of cables not directly connected to the electrical source is strictly prohibited.

4.2 LOAN OF ICT EQUIPMENT

The following are procedures on the loan of ICT equipment :

4.2.1 All ICT equipment loan must be in accordance to the procedure specified by the University.

4.2.2 All ICT equipment loan must be recorded and the following details must be included:

4.2.2.1 Borrower's details

4.2.2.2 Loan Period

4.2.2.3 Reason for borrowing

4.2.2.4 Details of loan approval

4.2.3 In case of damage or missing ICT equipment loaned by the university, the borrower must immediately report the matter to the University.

4.2.4 The borrower is responsible for the security of the ICT equipment (virus, software system and others) throughout the loan period.

4.2.5 Student wishing to borrow ICT equipment should do so through a university staff.

4.2.6 In the case of missing loaned ICT equipment, the matter must go through the Standardization of Lost University Assets Committee (Jawatankuasa Pelarasan Kehilangan Harta Universiti) by submitting a Police Report to the University Security Department and Facility Management.

4.2.7 The University has the right to withdraw any loan at any time if:

4.2.7.1 University guideline has been broken.

4.2.7.2 The equipment is required for University need.

4.2.8 Loans are given based on the availability of equipment.

4.3 THE RETURN OF ICT EQUIPMENT

4.3.1 The borrower should return the equipment on the specified date. If the borrower fails to do so, action will be taken by CICT management.

4.3.2 ICT equipment must be returned in good condition, functional and complete.

5 GUIDELINES

5.1 Users are advised to program a password in a computer if the computer contains confidential University data that cannot be disclosed to others.

5.2 Users must ensure that computer equipment is always in good, clean condition and properly maintained.

5.3 Users must use computer equipment provided by the university ethically.

H. PROCEDURES ON THE DISPOSAL OF THE ICT EQUIPMENT

1 INTRODUCTION

Disposal is a process of removing assets under ownership, control, supervision and in the records according to the stipulated procedure. ICT equipment includes all hardware or physical component and software in a particular computer system.

2 OBJECTIVE OF PROCEDURE

The aim of the procedure is to provide a reference point for all staff at different Faculties/Centres /Departments/Units with regard to the disposal of ICT equipment.

3 SCOPE OF PROCEDURE

The criteria and justifications for the disposal is in accordance to the Treasury Circular No. 5/2007 and UTM Treasury Circular No. 2/2007. The following aspect must be taken into consideration for the disposal of ICT equipment:

3.1 The capability and/or the efficiency of the equipment are low and becoming increasingly low in comparison to the task demand.

3.2 Obsolete equipment or equipment unable to fulfill the current requirement due to technological change.

3.3 High cost of maintenance and/or operational cost but low efficiency of equipment.

3.4 High frequency of error.

3.5 Supply agent or company seize offering service and support for the particular equipment.

3.6 The unavailability or difficulty of obtaining spare parts.

4 DISPOSAL OF ICT EQUIPMENT

4.1 ICT equipment should be disposed of according to current UTM procedure on the disposal of ICT equipment.

4.2I CT equipment include hardware supplied by CICT or the University.

5 GUIDELINE

5.1 Disposal procedure should be done by in controlled manner and complete so that all information are under the control of the university.

5.2 Precautionary measure must be taken before disposal is implemented. This includes eliminating all data content in equipment especially official secret information before it is disposed.

5.3 Lifetime guideline:

5.3.1	Computer	-	4 years
5.3.2	Printer	-	4 years
5.3.3	Notebook	-	4 years
5.3.4	Scanner	-	4 years
5.3.5	LCD Projector	-	4 years
5.3.6	Monitor	-	4 years
5.3.7	Server	-	4 years

5.4 Disposal / Repair:

5.4.1. ICT devices not reaching their lifetime can be disposed if the cost of repair exceeds 50% of the cost of new equipment.

I. PROCEDURES FOR ICT SECURITY

1 INTRODUCTION

Amongst the major challenges in provide services with high availability and integrity are handling issues related to intrusion, hacking, denial of service both intentionally and unintentionally and data espionage. The university has invested heavily to increase level of security for the ICT's service delivery. Nevertheless human factor and process still are factors which to be given priority at this point in time.

2 OBJECTIVES OF PROCEDURE

The objective of the procedure is

2.1 To ensure the secure control and management of computer hardware, software, application and operation and

2.2 To give details of the implementation of the secure in campus online network system that forms the local area network (LAN) for the purpose of communication and data sharing

3 SCOPE OF PROCEDURE

The scope covered includes

3.1 The security aspect of the hardware, software system, data server and application system and

3.2 The security system aspect of the internet access.

4 RESTRICTED PHYSICAL ACCESS

4.1 Cable protection in public area through the installation of conduit or other protective mechanism

4.2 Restricted access to the computer server room and also access to all servers and other ICT sources and

4.3 Restricted physical access to staff and individuals to access the servers

5 RESTRICTED LOGICAL ACCESS

Monitoring access is carried out during installation to ensure that only authorized personnel has access to the system mechanism.

6 USER IDENTIFICATION

User includes individual user or group of users that share a group account. Both types of user must be responsible for the security of the system. Steps taken to verify authorized user are as follows:

6.1 Assigning a unique ID for each individual user

6.2 Recording and monitoring all user ID responsible for every activity

6.3 Ensuring the availability of auditing facility to check user activity

6.4 Ensuring all user ID created is based on application and there is no user ID that is unused

6.5 Changing User ID for system application purposes must obtain permission from the system owner.

6.6 The following steps are taken in order to ensure inactive user ID is not misused:

6.6.1 Withdrawing all privileges of users whose ID are found inactive for a continuous period of 30 days and terminating the user ID after the 30 day period and

6.6.2 Terminating all user privileges for users who have moved or ended their service.

6.7 Audit trail carried out on every user activity is recorded and archived if there is adequate storage capacity. This is especially important to identify users who have accessed confidential data in cases where data trespass has been committed.

6.8 User Verification

The verification process aims to ensure that only authorized users are allowed to use the system via a valid password. The system must be able to demonstrate the following capabilities

6.8.1 Password entered must not be displayed

6.8.2 Password must contain at least 8 characters

6.8.3 Password must be a combination of number, alphabet and symbol-

6.8.4 Passwords are encrypted when transferred

6.8.5 Password file is kept separate from the main application data and

6.8.6 Access attempt is limited to three (3) times only. User ID will be suspended after three (3) continuous failed attempts.

7 AUDIT TRAIL

7.1 The University is responsible for creating and storing the audit trail record for identifying user accountability and security.

7.2 The use of an audit trail for a computer system and manual operation must be created for:

7.2.1 Accessing critical information

7.2.2 Accessing the network service and

7.2.3 Using special privileges or gaining special access which exceed access given to regular user such as security command and super-user function.

7.3 Audit trail information includes the following

7.3.1 User identification (ID)

7.3.2 Function, source and information used or updated

7.3.3 Date and time of use

7.3.4 Client's IP address or work station and

7.3.5 Specific transaction and program executed.

7.4 The University will carry out the following while creating an audit trail:

7.4.1 Monitor and immediately report any suspicious activity

7.4.2 Carry out scheduled monitoring of audit trail

7.4.3 Monitor and report all security related problems and irregular activities

7.4.4 Store audit trail data for a particular time period for operational and security purpose and

7.4.5 Protect audit trail data from modification, deletion, deception, or reprogrammed.

8 INFORMATION BACKUP

8.1 The University is responsible for completely restoring the system in case of break down or damage

8.2 Back up process is carried out according to schedule and during system configuration change. Backup is separately and securely stored.

8.3 The University will take the following course of action when creating back up:

8.3.1 Documenting backup and restore procedures

8.3.2 Storing three (3) backup generation and

8.3.3 Testing media backup and restore procedure twice (2) a year.

9 MAINTENANCE

9.1 The University will carry out monitoring and maintenance to ensure the integrity of operational system from any security threat or breach:

9.1.1 Patches and Vulnerabilities - Updating patches and overcoming vulnerabilities that occur from the registered security agent

9.1.2 Upgrading – upgrading operational system to the latest version suitable to the specification of the ICT equipment.

10 APPLICATION OF SECURITY SYSTEM

The University is responsible for carrying out and controlling the access level of the application system.

11 SOFTWARE APPLICATION

11.1 Security monitoring is carried out to prevent unauthorized access, modification, and exposure or data deletion. The university is responsible for creating the following restriction and facilities:

11.1.1 Central security system with controlled access via a single user ID and password for all

11.1.2 Profile access that limits access to data and function according to user category

11.1.3 Using second level authentication (such as smart card) for mission critical applications to increase level of integrity

11.1.4 System application level monitoring to verify specific user accountability and

11.1.5 Specification of data ownership.

12 DATABASE

12.1 The University is responsible to create restrictive access to the database. The integrity of the information stored in the database is maintained and guaranteed through:

12.1.1 Database management system that ensures the integrity of information update and access and

12.1.2 Access to information is determine by the Database Administrator

13 APPLICATION TESTING

13.1 The University is responsible to test the program, module, application system and the integration of the application system to ensure that the system is functioning according to its specification. The following steps are taken during application testing:

13.1.1 Using testing data (dummy) or historical data

13.1.2 Controlling the use of classified data

13.1.3 Limiting the access to relevant staff only

13.1.4 Removing information after completing test (especially when historical data is used) and

13.1.5 Using separate environment for creating and operating application system.

14 MALICIOUS AND DEFECTIVE SOFTWARE

14.1 Application system programs are exposed to malicious and defective codes. The university is responsible to minimize the probability of defective software through the following:

14.1.1 Using source code from an application system developer that is reputable, possess good service track record and high technical expertise

14.1.2 Creating and carrying out quality assurance program and procedure on all locally and externally developed application systems

14.1.3 Ensuring all application systems are documented, tested, undergone function and robustness verification and have fulfilled the specification.

15 VERSION CHANGE

15.1 The university is responsible to control the version application system when modification or upgrading is carried out and to ensure that control procedure is strictly adhered to.

16 SOURCE CODE STORING

16.1 The University is responsible to manage and carry out a controlled source code storing for application system developed locally and externally for maintenance and upgrading purposes which include the following:

16.1.1 Creating an up to date a maintenance procedure and

16.1.2 Creating an agreed scenario in case of damaged and disaster and source code is unavailable.

17 UNLICENSED SOFTWARE

17.1 The University is responsible to make certain that all software used is licensed, and to control the storage and physical access to the licensed software and copy of the issued license.

18 MALICIOUS CODE CONTROL

18.1 The University is responsible in ensuring the following steps are taken to maintain information integrity and protect it from exposure and destruction due to malicious code:

18.1.1 Implement procedure on malicious code management

18.1.2 Create guideline with regard to software download, acceptance and use of freeware and shareware

18.1.3 Distribute instruction and information on how to detect malicious code to all users and

18.1.4 In case of malicious code attack, take the following precautionary or remedial steps:

18.1.4.1 Scan and destroy malicious code using recognized antivirus software

18.1.4.2 Verify status scanning process in the log report and

18.1.4.3 Do not run or open attachment from suspicious email

19 SECURE EMAIL USE

(refer to procedure to use e-mail)

20 SECURITY OF NETWORK EQUIPMENT

All equipment that will be installed must satisfy the Factory Acceptance Check (FAC) before installation and configuration.

21 PHYSICAL SECURITY

21.1 Network equipment must be placed in a location free from unexpected risks such as flood, lightning, tremor, filth and others

21.2 The air conditioning system must be constantly operated to ensure that the temperature of the network equipment is at a controlled level.

21.3 Uninterruptible Power Supply (UPS) is installed with a minimum 15 minutes operation in case of power failure or lightning and to support automatic server shut down.

22 PHYSICAL ACCESS SECURITY

22.1 The following are steps that should be taken to ensure the protection of network cables from unauthorized access:

22.1.1 Protecting cabling in public area through the installation of conduit or other protective mechanism and

22.1.2 Locating central wiring closet in a secure area or room with limited access by authorized personnel only

23 NETWORK EQUIPMENT ACCESS

23.1 Equipment must be placed in a secure and controlled area and

23.2 Network equipment can only be accessed by authorized personnel.

24 LOGICAL ACCESS

24.1 User ID and password is required to gain access to network software. Access can only be made by authorized personnel

24.2 Password composition must be in line with the stipulated guideline

24.3 Access information to the router must be recorded – personnel name, date, time and activity. Information must be stored for at least 90 days

24.4 Network can only accept traffic from registered local IP address. All network switch configuration changes must be logged including date and time change by user

24.5 Software configuration change must be recorded – personnel carrying out change, personnel authorizing change and the date and

24.6 Configuration change must be centrally executed.

25 UNAUTHORIZED EQUIPMENT USE

25.1 Equipment other than authorized are not to be connected

25.2 Wiring closet can only be accessed by authorized personnel

26 EQUIPMENT CONFIGURATION

26.1 Enabling only required services

26.2 Limiting configuration access to authorized node or IP address

26.3 Disabling traffic broadcast

26.4 Using secure password and

26.5 Performed by trained and authorized personnel only

27 EQUIPMENT MAINTENANCE

27.1 Equipment must be installed, operated and maintained according to the manufacturer's specification

27.2 Equipment must be repaired and maintained by trained and authorized personnel only and

27.3 Maintenance record must be updated.

28 USER ACCESSIBILITY TO CARRY DATA RECONNAISSANCE

28.1 Software sniffer or network analyzer is prohibited from using any computer without consent from the CICT Director or ICT Security Officer.

29 NOT RECOMMENDED NETWORK PROTOCOLS

29.1 Using network protocol that requires high bandwidth such as NetBIOS and IPX/SPX and

29.2 Workgroup usage to support share-level security

30 FIREWALL

30.1 All inward and outward UTM network traffic must be filtered by firewall and only authorized traffic will be allowed.

30.2 Firewall configuration must take into account the following:

30.2.1 Audit and archive requirement

30.2.2 Availability

30.2.3 Confidentiality and

30.2.4 UTM information protection.

30.3 Authorized units with designated computer server can configure specific firewall for security purposes.