

	IT Services		Sunway University College		
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 1 of 6

## SYUC e-POLICY

### 1. PURPOSE

The purpose of the e-Policy is to ensure that **Sunway University College (SYUC)** computer resources are used properly by its **Users**. The rules and obligations in this Policy apply to all Users of SYUC's computer network, systems, devices and services wherever they may be located. Violations will be taken seriously and may result in disciplinary action, including termination, and civil and criminal liability.

It is every User's duty to use SYUC's **Computer Resources** responsibly, professionally, ethically and lawfully.

### 2. DEFINITIONS

"**Sunway University College**" or "**SYUC**" means Sunway University College and its Group of Colleges.

The term "**Computer Resources**" refers to SYUC's entire computer systems, network and services, which include & not limited to: Host Computers, File Servers, Application Servers, Network Communication Servers, Mail Servers, Fax Servers, Web Servers, Workstations, Stand-alone Computers, Laptops, Software, Data Files, all internal and external computers and communication networks (eg. Internet, Commercial Online Services, Value-added Networks, Email Systems), computer peripherals (eg. Printers, Scanners, Projectors, Zip Drives, CD Roms, CD Writers, Pen-drives, UPS, etc) and network equipments (eg. Network Cables, Hubs, Switches, Routers, Bridges, PacketShapers, Network Interface Cards, Wireless Network Cards, Wireless Access Points, etc.) that may be accessed directly or indirectly from SYUC computer network.

The term "**Users**" refers to all staff and students, contract staff and other persons or entities who use the Computer Resources.

### 3. POLICY

The Computer Resources are property of SYUC and may be used only for legitimate business purposes. Users are permitted access to the Computer Resources to assist them in performance of their jobs and for teaching and learning purpose. Usage of Computer Resources can be revoked at any time.

In using or accessing SYUC Computer Resources, Users must comply with the following provisions:

#### 3.1 PROHIBITED ACTIVITIES

##### 3.1.1 Inappropriate Or Unlawful Material

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, rumors in nature, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as e-bulletin board systems, newsgroups, chat groups, Web Telecommunication Kiosk, Vine Announcement Messages) or displayed on or stored in SYUC's computers.

##### 3.1.2 Prohibited Uses

Users are not to use SYUC's Computer Resources for dissemination or storage of commercial or personal advertisements, solicitations,

	IT Services		Sunway University College		
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 2 of 6

promotions, destructive programs (ie viruses or self-replicating code) or any other non-work and non-academic related use.

### 3.1.3 Waste Of Computer Resources

Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include but are not limited to, sending mass mailings or chain letters, email spamming, spending excessive amount of time on the Internet, playing games, engaging in online chat groups, printing non-work related documents, probing/hacking company system or otherwise creating unnecessary network traffic.

### 3.1.4 Misuse Of Software

Without prior written authorization from SYUC ITS, Users may not do any of the following:

- Copy software for use on any computer.
- Provide copies of software to any independent contractors or clients of SYUC or to any third party.
- Install software on any of SYUC's workstations or servers.
- Download any non-work or academic related software from the Internet or other online service to any of SYUC's workstations or servers.
- Modify, revise, transform, recast or adapt any software.
- Reverse-engineer, disassembles or recompiles any software.

Users may not violate terms of applicable software licensing agreement or copyright laws. Users who become aware of any software misuse should report to SYUC ITS immediately.

### 3.1.5 Communication Of Trade Secrets

Unless expressly authorized, sending, transmitting or otherwise disseminating proprietary data, trade secrets or other confidential information of the company is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties including but not limited to Computer Crimes Act 1997.

### 3.1.6 Mishandling of Computer Hardware

Users may not undertake activities like dismantling, alteration, modification, repairing of SYUC computer hardware resources. Such services will be provided by SYUC's ITS staff or agents appointed by ITS.

### 3.1.7 Personnel Hardware & Software

	IT Services		Sunway University College		
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 3 of 6

Without prior approval from ITS, private owned hardware and software are not allowed to be connected to the local area network or be attached to any equipment which is connected to the network.

### 3.2 ACCOUNTS & PASSWORDS

#### 3.2.1 Responsibility For Accounts & Passwords

Users are responsible for safeguarding their accounts & passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their accounts & passwords. No User may access computer system with another User's password or account. Masking the identity of an account or machine is also prohibited.

#### 3.2.2 Passwords Do Not Imply Privacy

Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system.

Users expressly waive any right of privacy in anything they create, store, send or receive on the computer or through the Internet or any other computer network. Users consent to allowing authorised personnel of SYUC to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that SYUC may use human or automated means to monitor use of its Computer Resources.

### 3.3 SECURITY

#### 3.3.1 Accessing Other User's Files

Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file unless such file is posted in the Team Rooms or Network Shared drives for sharing and discussion purposes. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and e-mail.

#### 3.3.2 Accessing Other Computers & Networks

A User's ability to connect to other computer systems through the network (wired or wireless) or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by SYUC ITS.

#### 3.3.3 Computer Security

Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of SYUC's Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing SYUC's network without authorization and to prevent introduction and spread of viruses.

#### 3.3.4 Security Interference

	IT Services		Sunway University College		
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 4 of 6

The user may not knowingly perform an act, which will interfere with the normal operation of computers, terminals, peripherals, or networks. Users are prohibited to run or install on any computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer system, or network. The user may not attempt to circumvent data protection schemes or uncover security loopholes.

### 3.4 VIRUSES

#### 3.4.1 Virus Detection

Viruses can cause substantial damage to computer systems. It is the responsibility of each & every user to ensure installation of the latest version of approved anti-virus software. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into SYUC's network.

To that end, all material received on diskette or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to SYUC MUST be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to SYUC's network must be scanned for viruses.

#### 3.4.2 Accessing The Internet

To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to SYUC's network must do so through SYUC's Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless the computer you are using is not connected to the company's network or with written approval from SYUC ITS.

Use of the Internet must be utilized with common sense and good judgment. If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible termination.

### 3.5 DISCIPLINARY ACTIONS

#### 3.5.1 Minor

Minor infractions of this policy or those that appear accidental in nature are typically handled internally in an informal manner by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

#### 3.5.2 Serious

Serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of campus policies, or repeated violations of minor infractions, may result in the temporary or permanent loss of access privileges. In all cases, the offender's associated school or department will be notified of

	IT Services			Sunway University College	
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 5 of 6

the infraction. If the offender is a student at the College, the case will also be referred to the College Management for appropriate action.

### 3.5.3 Offences

Offences that are in violation of local, state, or federal laws will result in the immediate loss of computing privileges, and will be reported to the appropriate SYUC and law enforcement authorities. Users are advised to adhere to the Malaysian Cyberbills as follows:-

- Computer Crimes Bill 1997
- Copyright (Amendment) Bill 1997
- Digital Signature Act 1997
- Telemedicine Bill 1997
- Communications and Multimedia Act 1998
- Digital Signature Regulations 1998

SYUC reserves the rights to modify or discontinue, temporarily or permanently, the computer systems access with or without notice to user. Users agree that SYUC shall not be liable for any modification or discontinuance of access rights to the computer systems.

Any user who discovers a violation of this policy shall notify SYUC ITS. Any such report will be classified as private and confidential.

## 3.6 MISCELLANEOUS

### 3.6.1 Use Of E-Mail

Think before sending a message. It is very important that you use the same care and discretion in drafting e-mail as you would for any other written communication.

Material that is fraudulent, harassing, offensive, embarrassing, sexually explicit, profane, obscene, intimidating, disruptive, rumors in nature, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail.

Chain e-mail is a message sent to a number of people asking each recipient to send copies with the same message to a specified number of others. Do not forward or initiate chain e-mail. Users who fail to comply with these guidelines may be subject to disciplinary action, including revocation of e-mail privileges.

### 3.6.1 Compliance With Applicable Laws & Licences

In the use of Computer Resources, Users must comply with all software licenses, copyrights and all other laws governing intellectual property and online activities.

Users must also observe and comply with all policies and guidelines of SYUC.

### 3.6.2 SYUC Rights

SYUC reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the computer systems. Files may be subject to search under court order. In addition, system administrators

	IT Services		Sunway University College		
	Title	SYUC e-Policy		Ver	1.1
				Date	01 Aug 2005
Owner	OMLoo	Code	DOC/e-Policy		Page 6 of 6

may access user files or examine files or accounts that are suspected of unauthorized use or misuse, or that which may have been corrupted or damaged. All files and email messages transmitted by, received from, or stored in SYUC computer systems are the property of SYUC.

3.6.3 Amendments & Revisions

This Policy may be amended or revised from time to time as the need arises. Users will be informed through the SYUC's Intranet on all amendments and revisions.

3.6.4 No Additional Rights

This Policy is not intended to and does not grant Users any contractual rights. This Policy also does not grant SYUC's appointed Systems Administrator any right to access and view the files and databases meant for other colleagues through the use of Administrator Password unless with written authorization from the ITS Manager.

3.6.5 Policy Administrator

SYUC ITS Manager will be responsible to administer the E-Policy.

3.6.6 Violations Of E-Policy

Any violation of this Policy will be taken seriously and may result in disciplinary action, including termination as well as civil or criminal liability being taken against Users.