University Malaysia of Computer Science & Engineering

Acceptable Use Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 1 of 8

University Malaysia of Computer Science & Engineering is hereinafter referred to as "the university".
University network & internet access infrastructure is hereinafter referred to as "UniMyNet".

1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to staff and students for performance of their job functions and accessing internet data. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the UniMyNet. This policy explains how universty information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using university resources. Questions on what constitutes acceptable use should be directed to the user's Head of CIT.

2.0 Purpose

Since inappropriate use of UniMyNet exposes the university to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of university information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of university CSIT resources, including but not limited to, computer systems, email, the network, and the UniMyNet.

4.0 Policy

4.1 E-mail Use

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the university network, and B) such usage does not negatively impact the user's job performance.

• The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

• The user is prohibited from forging email header information or attempting to impersonate another person.

• Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the university may not be sent via email, regardless of the recipient, without proper encryption.

• It is university policy not to open email attachments from unknown senders, or when such attachments are unexpected.

• Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that detailed information about the use of email may be covered in the university's Email Policy.

4.2 Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-users of the university, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

4.3 Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use

The following actions shall constitute unacceptable use of the UniMyNet. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the UniMyNet and/or systems to:

• Engage in activity that is illegal under local, state, federal, or international law.

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the university.

- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

- Engage in activities that cause an invasion of privacy.

- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

- Make fraudulent offers for products or services.

- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of university user's job function.

- Install or distribute unlicensed or "pirated" software.

- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.5 Blogging and Social Networking

Blogging and social networking by the university's employees are subject to the terms of this policy, whether performed from the UniMyNet or from personal systems. Blogging and social Networking are allowed from the UniMyNet provided that A) it is done in a professional and responsible manner, B) confidential data is not disclosed, C) it does not impact the user's job performance, and D) no information detrimental to the university is published. The user assumes all risks associated with blogging and/or social networking.

4.6 Instant Messaging

Instant messaging is allowed such that it follows guidelines on disclosure of confidential data and does not negatively impact the user's job function.

4.7 Overuse

Actions detrimental to the UniMyNet or other university resources, or that negatively affect job performance are not permitted.

4.8 Web Browsing

The Internet is a network of interconnected computers of which the university has very little control. The employee should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The university is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Personal Use. The university recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of university computer systems to access the Internet is permitted during lunch, breaks, and before/after operation hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the university or on the user's job performance.

4.9 Copyright Infringement

The university's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.10 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is allowed as long as illegal and/or copyrighted materials are not downloaded or shared, and as long as it does not negatively impact the computer network or the user's job performance.

4.11 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

4.12 Monitoring and Privacy

Users should expect no privacy when using the UniMyNet or university resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The

university reserves the right to monitor any and all use of the computer network. To ensure compliance with university policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.13 Bandwidth Usage

Excessive use of university bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low university-wide usage.

4.14 Personal Usage

Personal usage of university computer systems is permitted during lunch, breaks, and before/after operation hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the university or on the user's job performance.

4.15 Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as it is provided by the university. Remote access to the network must conform to the university's Remote Access Policy.

4.16 Circumvention of Security

Using university-owned or university-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities

No university-owned or university-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing

- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
- Downloading, storing, or distributing copyrighted material

The university will take all necessary steps to report and prosecute any violations of this policy.

4.18 Non-University-Owned Equipment

The user must obtain written permission from the Head of Campus IT before installing outside or non-university-provided computer systems on the university network. Once this permission is obtained, and dependent on any conditions granted along with such permission, the user can connect a non-university-owned system to the network. Reasonable precautions must be taken to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the university network.

4.19 Personal Storage Media

The university does not restrict the use personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the UniMyNet provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the university network. Use of personal storage media must conform to the university's Mobile Device Policy.

4.20 Software Installation

No non-university-supplied software is to be installed without written permission of the IT Manager. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. For these reasons, installation of non-university-supplied programs is strongly discouraged. If a certain program is required for his or her job function, the user should contact the Campus IT Department to request permission.

4.21 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the university Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains university information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact the university's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 Applicability of Other Policies

This document is part of the university's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Head of Campus IT and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

6.0 Definitions

Blogging The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

7.0 Revision History

Revision 1.0, 01/04/2013