Information Security Management System
ISO/IEC 27001:2013

RULES AND REGULATIONS REGARDING ICT FACILITIES

PERATURAN DAN KAEDAH BERKAITAN KEMUDAHAN ICT

For PTM Use Only	Version 1.0	Date: 6th Oct 2015
Written By: Asiah Abu Samah Pengerusi Jawatankuasa ISMS	**Verified By:** Haslina Abd Hamid Wakil Pengurusan Keselamatan Maklumat (ISMR)	**Approved By:** ICt Council

Revision History

No	Date of Change	Description	Page	Version	Approved By

1.0 Introduction

As a proof of University of Malaya's (UM) commitment to the development and the use of new Information and communications technology (ICT), all users who use UM's ICT facilities are allowed to use the Internet and Intranet. Rules and Regulations Regarding ICT Facilities is designed to help UM to inspire users to understand their use does not conflict with law, protect the UM from any ICT threat as well as how to use these resources as best as possible.

2.0 Scope

The rules and regulations applies to all users of UM's ICT facilities.

However, the scope for ISMS audit and certification only covers desktop computer, laptops and servers belonging to Pusat Teknologi Maklumat (PTM) and located in PTM premises.

3.0 Objectives

3.1. Explain to users the matters that must be observed and avoided when using the UM's ICT Facilities.

3.2. Protect the users and the UM's ICT facilities from any risk of ICT security threats, including and not limited to virus attacks and malicious code, misuse of ICT assets and any legal issues.

4.0 Rules

Access to Facilities

4.1. If you connect any device (wired or wireless) to the University network, you MUST abide by all terms contained in the University Rules and Regulations Regarding ICT Facilities and any policies and guidelines governing them. The rules must be agreed by users when they register for the UM ID or identification.

4.2. Access to the University network may be suspended or terminated if you are in violation of any of these Rules and Regulations. Notwithstanding this, you may also be subject to disciplinary action under the Laws Of Malaysia Act 30, Universities and University Colleges Act 1971. Reinstatement of computer facilities is subject to an appeal to the Chief Information Officer (CIO).

4.3. In order to use the University's Information Systems and access the wireless network you must create a UM's official ID (email) through an online form and affirm your ICT Declaration.

Use of Facilities

4.4. By using the UM's ICT facilities or connecting any equipment to the University network, you agree to abide by all University Rules and Regulations. It is your responsibility to stay up-to-date with these Rules and Regulations.

4.5. You should not knowingly create, transmit, receive or handle any material on UM's ICT facilities that may be offensive to any employee and student of the University or the public. Any attempt to access UM's ICT facilities or another user's computer, account or e-mail; or impersonate as another user or create or introduce programs with malicious intent; or involve in software theft; or use UM's ICT facilities to harass any company or individual; or send chain or junk mail, may result in appropriate action by the University.

4.6. The UM network and all UM's ICT facilities are for official use only.

You MUST :

a) obtain written permission from the CIO before running any unauthorised services that can lead to security vulnerabilities and can cause connection problems for you and other network users.

b) be responsible for the use of all ICT resources allocated to you. Therefore, sharing an account is prohibited.

c) respect the privacy of other user. You are prohibited from accessing or copying other users' email, data, program or file without their permission.

d) keep your passwords secure. Do not disclose them to, or allow them to be used by any other person.

e) ensure your computer/device be kept up-to-date with operating system updates and security patches. Failure to install system and security patches may leave your computer vulnerable to viruses, malware and malicious attacks which could result in your computer being disconnected from the network.

f) ensure your computer have up-to-date anti-virus software that updates automatically from a trusted software vendor. You will be disconnected from the network if your computer becomes infected with viruses, malware or if it displays suspicious network activity.

g) ensure the security of your devices / notebooks / PCs. You may seek help from the IT officer of your department or PTM.

h) comply with all the internal laws of the University and the national laws governing the use of ICT facilities, whether directly or indirectly.

You **MUST NOT**:

a) attempt to access or alter restricted portions of the operating system in the computer (e.g. registry) or configuration (e.g. IP Address, Computer Name and Active Directory settings) in the computer room facilities unless authorized by the appropriate University's representative (Wakil ICT). You are required to take reasonable care of these facilities and report faults immediately to the respective representative.

b) use a computer that is not provided to you without the consent of the owner or administrator of the system (exception: computers for public use).

c) make any attempt to damage or destroy hardware, software or data in other computers (vandalism) over the network. This includes but is not limited to spreading viruses.

d) alter or destroy data belongs to other users.

e) use the campus network resources to launch attacks on computers, accounts or other users by spreading viruses, worms, trojan or other malicious code to other computers either within or outside UM.

f) connect any wireless access point, cable/broadband router, hub, switch, game console or any such devices to the UM network without written permission from the CIO.

g) use any file-sharing software or participate in Peer-to-Peer (P2P) file-sharing networks unless prior written permission is obtained from the CIO. The file-sharing networks may include, but is not limited to, Kazaa; Napster; Gnutella; Morpheus; iMesh; Grokster; Limewire; NEOnet; Oxtella; Edonkey; eMule; Undernet; Bit Torrent; Aimster; WinMX; and Azureus. If you are found to have P2P software running on your computer you will be subject to appropriate action by the University.

h) illegally run security scan on system. Scans are considered dangerous and unethical actions.

i) use campus ICT resources to disrupt or threaten the safety of others

j) perform an action that could interfere computers, peripheral devices or network daily operations.

k) run or install any program that cause damage or congestion to the computer or network.

l) for any reason build, install or spread computer viruses, Trojan horses or other malicious code to computers belong to university or network facilities.

m) perform any attempt to damage the system or expose the weaknesses of data protection security system. This includes developing or using programs designed to identify system weaknesses and security or illegally de-encrypt encrypted data.

n) prepare, upload, download, save, store or use any material containing pornographic elements, unlicensed software and other applications such as electronic games, video and music which will interfere with the normal operation of computers, terminals, peripherals, or networks.

Monitoring and securing the network

4.7. PTM has the right to log all network traffic in order to detect problems and to ensure the network is operating correctly. The logs record may include, but is not limited to, usernames, MAC addresses, IP addresses of clients and servers, traffic type, application classification and amount of data transferred.

4.8. In the event of a network fault, or a case of serious network abuse (from within the University or from outside), it may be necessary to actively record certain network traffic. This is done only to record particulars under investigation, and will be restricted to just the activities of a computer or any service.

4.9. Any investigation into network use will be done when necessary. User under investigation shall have the right to a fair hearing and given an opportunity to submit any written representation.

4.10. The University occasionally runs network scans to detect any unauthorised devices or services or any security vulnerabilities to protect the University network and its users. If any unauthorised devices or services are detected, the University will contact the owner of the computer. You are required to ensure that your computer's name that was set by PTM staff or Wakil ICT PTj is not changed to enable the University to identify it and provide any assistance.

4.11. The University has installed firewalls to prevent unauthorised access to the network and services. You may contact PTM should there be any interference in your use of the University network.

1.0 Pengenalan

Sebagai bukti komitmen Universiti Malaya (UM) untuk pembangunan dan penggunaan Teknologi Maklumat dan Komunikasi (ICT) yang baru, semua pengguna yang menggunakan kemudahan ICT UM dibenarkan menggunakan Internet dan Intranet. Peraturan dan Kaedah Berkaitan Kemudahan ICT ini direka bagi membantu UM untuk memberi inspirasi kepada pengguna dalam memahami penggunaannya supaya tidak bercanggah dengan undang-undang, melindungi UM dari sebarang ancaman ICT serta kaedah bagaimana untuk menggunakan sumber-sumber ini dengan sebaik mungkin.

2.0 Skop

Peraturan dan kaedah ini terpakai kepada semua pengguna kemudahan ICT UM.

Walau bagaimanapun, skop audit dan pensijilan ISMS hanya meliputi komputer meja, komputer riba dan pelayan yang dimiliki oleh Pusat Teknologi Maklumat (PTM) yang berada di premis PTM.

3.0 Objektif

3.1. Menerangkan kepada pengguna perkara yang perlu diambil tindakan dan dielakkan semasa menggunakan kemudahan ICT UM.

3.2. Melindungi pengguna dan kemudahan ICT UM dari sebarang risiko ancaman keselamatan ICT, termasuk dan tidak terhad kepada serangan virus dan kod berniat jahat, penyalahgunaan aset ICT dan mana-mana isu-isu undang-undang.

4.0 Peraturan

Akses kepada kemudahan

4.1. Jika anda menyambung mana-mana peranti (berwayar atau tanpa-wayar) ke rangkaian Universiti, anda MESTI mematuhi semua syarat-syarat yang terkandung di dalam peraturan dan kaedah ini dan apa-apa dasar dan garis panduan yang mengawal mereka. Peraturan dan kaedah ini mesti dipersetujui oleh pengguna apabila mereka mendaftar untuk ID atau pengenalan UM.

4.2. Akses kepada rangkaian Universiti boleh digantung atau ditamatkan jika anda melanggar mana-mana perkara dalam peraturan dan kaedah ini. Walau bagaimanapun, anda juga mungkin dikenakan tindakan disiplin di bawah Akta 30 Undang-Undang Malaysia, Akta 1971 Universiti dan Kolej Universiti.

Pengembalian semula kemudahan komputer adalah tertakluk kepada rayuan kepada Ketua Pegawai Maklumat (CIO).

4.3. Untuk menggunakan Sistem Maklumat Universiti dan mengakses rangkaian tanpa-wayar, anda perlu membuat ID rasmi UM (e-mel) melalui borang dalam talian dan mengesahkan Deklarasi ICT anda.

Penggunaan Kemudahan

4.4. Dengan menggunakan kemudahan ICT UM atau menyambung mana-mana peralatan ke rangkaian Universiti ini, anda bersetuju untuk mematuhi semua peraturan ICT Universiti. Adalah menjadi tanggungjawab anda untuk mengetahui peraturan ICT yang terkini.

4.5. Anda tidak patut, samada secara sengaja atau tidak sengaja, membuat, menghantar, menerima atau mengendalikan apa-apa bahan di kemudahan ICT UM yang mungkin menyinggung perasaan mana-mana kakitangan dan pelajar Universiti atau orang awam. Sebarang percubaan untuk mengakses kemudahan ICT atau komputer pengguna UM lain, akaun atau e-mel; atau menyamar sebagai pengguna lain atau mencipta atau memperkenalkan program dengan niat jahat; atau terlibat dalam kecurian perisian; atau menggunakan kemudahan ICT UM untuk mengganggu mana-mana syarikat atau individu; atau menghantar emel rantai atau sampah, boleh menyebabkan tindakan yang sewajarnya oleh pihak Universiti.

4.6. Kemudahan rangkaian dan semua kemudahan ICT UM adalah untuk kegunaan rasmi sahaja.

Anda MESTI

a) mendapatkan kebenaran bertulis daripada CIO sebelum menjalankan apa-apa perkhidmatan yang tidak dibenarkan yang boleh membawa kepada kelemahan keselamatan dan boleh menyebabkan masalah sambungan ke rangkaian untuk anda dan pengguna lain.
b) bertanggungjawab untuk penggunaan semua sumber ICT yang diberikan kepada anda. Oleh itu, berkongsi akaun adalah dilarang.
c) menghormati privasi pengguna lain. Anda adalah dilarang daripada mengakses atau menyalin e-mel, data, program pengguna lain atau fail tanpa kebenaran mereka.
d) memastikan kata laluan anda selamat. Jangan dedahkannya kepada, atau benarkan penggunaannya oleh orang lain.

e) memastikan komputer/peranti anda mempunyai *patch* sistem operasi dan *patch* keselamatan yang terkini. Kegagalan untuk memasang *patch* sistem dan keselamatan boleh menyebabkan komputer anda terdedah kepada virus, malware dan serangan berniat jahat yang boleh menyebabkan komputer anda diputuskan akses ke rangkaian.

f) memastikan komputer anda mempunyai perisian anti-virus terkini yang dikemas kini secara automatik dari perisian pembekal yang dipercayai. Akses ke rangkaian akan diputuskan dari rangkaian jika komputer anda dijangkiti dengan virus, malware atau jika ia memaparkan aktiviti rangkaian yang mencurigakan.

g) memastikan keselamatan peralatan / komputer riba / PC anda. Anda boleh mendapatkan bantuan daripada pegawai IT jabatan anda atau daripada pihak PTM.

h) mematuhi semua undang-undang dalaman Universiti dan undang-undang negara yang mengawal penggunaan kemudahan komputer, sama ada secara langsung atau tidak langsung.

Anda TIDAK DIBENARKAN

a) mencuba akses atau mengubah bahagian terhad sistem operasi di dalam komputer (contohnya *registry*) atau konfigurasi (contohnya Alamat IP, nama komputer dan tetapan *Active Directory*) dalam kemudahan bilik komputer melainkan jika dibenarkan oleh pihak pengurusan kemudahan ICT (spt wakil ICT). Anda dikehendaki menggunakan kemudahan ICT yang disediakan dengan baik dan melaporkan kerosakan dengan segera kepada wakil ICT masing-masing.

b) menggunakan komputer yang tidak diberikan kepada anda tanpa persetujuan pemilik atau pentadbir sistem (pengecualian: komputer untuk kegunaan awam).

c) membuat sebarang percubaan untuk merosakkan atau memusnahkan perkakasan, perisian atau data di komputer lain (vandalisme) melalui rangkaian. Ini termasuk tetapi tidak terhad kepada menyebarkan virus.

d) mengubah atau memusnahkan data milik pengguna lain.

e) menggunakan sumber rangkaian kampus untuk melancarkan serangan ke atas komputer, akaun atau pengguna lain dengan menyebarkan virus, cecacing, trojan atau kod berniat jahat ke komputer lain sama ada di dalam atau di luar UM.

f) Sambung mana-mana pusat akses tanpa-wayar, kabel/*broadband router*, hub, switch, konsol permainan atau mana-mana peranti kepada rangkaian UM tanpa kebenaran bertulis daripada CIO.

g) Gunakan mana-mana perisian fail perkongsian atau menyertai Peer-to-Peer (P2P) rangkaian perkongsian fail melainkan jika kebenaran bertulis diperolehi daripada CIO. Rangkaian perkongsian fail termasuk, tetapi tidak terhad kepada, Kazaa; Napster;

Gnutella; Morpheus; iMesh; Grokster; limewire; NEOnet; Oxtella; Edonkey; eMule; Undernet; Bit Torrent; Aimster; WinMX; dan Azureus. Jika anda didapati mempunyai perisian P2P *running* dalam komputer anda, anda akan dikenakan tindakan sewajarnya oleh Universiti.

h) menjalankan imbasan keselamatan pada sistem secara tidak sah. Imbasan dianggap tindakan berbahaya dan tidak beretika.

i) menggunakan sumber ICT kampus untuk mengganggu atau mengancam keselamatan orang lain

j) melakukan tindakan yang boleh mengganggu komputer, peranti periferal atau operasi harian rangkaian.

k) menjalankan atau memasang apa-apa program yang menyebabkan kerosakan atau kesesakan kepada komputer atau rangkaian.

l) untuk apa-apa sebab, membina, memasang atau menyebar virus komputer, kuda Trojan atau kod berniat jahat untuk komputer milik Universiti atau kemudahan rangkaian.

m) menjalankan sebarang percubaan untuk merosakkan sistem atau mendedahkan kelemahan sistem keselamatan perlindungan data. Ini termasuk membangunkan atau menggunakan program yang direka untuk mengenal pasti kelemahan dan keselamatan sistem atau de-encrypt encrypted data secara tidak sah.

n) menyedia, memuat naik, memuat turun, menyimpan, atau menggunakan apa-apa bahan yang mengandungi unsur-unsur lucah, perisian tidak berlesen dan aplikasi lain seperti permainan elektronik, video dan muzik yang akan mengganggu operasi normal komputer, terminal, peralatan, atau rangkaian.

Pemantauan dan keselamatan rangkaian

4.7. PTM mempunyai hak untuk log semua trafik rangkaian untuk mengesan masalah dan memastikan rangkaian beroperasi dengan betul. Log akan merekod termasuk tetapi tidak terhad kepada nama pengguna, alamat MAC, alamat IP pelanggan dan pelayan, jenis lalu lintas, klasifikasi permohonan dan jumlah data yang dipindahkan.

4.8. Sekiranya berlaku kerosakan rangkaian, atau kes penyalahgunaan rangkaian yang serius (dari dalam atau dari luar Universiti), trafik rangkaian tertentu mungkin perlu dirakam secara aktif. Ini dilakukan hanya untuk menyiasat butir-butir rekod dan ianya akan dihadkan kepada aktiviti-aktiviti komputer atau perkhidmatan sahaja.

4.9. Sebarang penyiasatan ke atas penggunaan rangkaian akan dilakukan apabila perlu. Pengguna di bawah siasatan mempunyai hak untuk perbicaraan yang adil dan diberi peluang untuk mengemukakan apa-apa representasi bertulis.

4.10. Universiti kadang-kadang menjalankan imbasan rangkaian untuk mengesan sebarang peranti atau perkhidmatan yang tidak dibenarkan atau sebarang kelemahan keselamatan untuk melindungi rangkaian Universiti dan penggunanya. Jika mana-mana peranti atau perkhidmatan yang tidak dibenarkan dikesan, pihak Universiti akan menghubungi pemilik komputer. Anda dikehendaki untuk memastikan bahawa nama komputer anda yang telah ditetapkan oleh kakitangan PTM atau wakil ICT PTj tidak berubah bagi membolehkan Universiti untuk mengenal pasti dan memberikan bantuan.

4.11. Universiti telah memasang firewall untuk menghalang capaian yang tidak dibenarkan kepada rangkaian dan perkhidmatan. Anda boleh menghubungi PTM sekiranya terdapat sebarang gangguan dalam penggunaan rangkaian Universiti.