Information Security Management System MS ISO/IEC 27001:2007

ACCEPTABLE USE OF IT ASSETS POLICY

DASAR PENGGUNAAN YANG DITERIMA PAKAI UNTUK ASET-ASET IT

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En. Farihan Ghazali	Pn. Rohazna Wahab Deputy Director ICT	En. Nasrudin Abd. Shukor Director ICT Division ISMR

For Dept Use Only

Date: 22nd March 2013 **Version 1.1**

Revision History

No	Date of Change	Description	Page	Version	Approved By
1.	22 Mac 2013	Nama asal Penulis Dokumen iaitu Pn Ummi Naiemah Saraih ditukar kepada En. Farihan Ghazali	0	1.1	Nasrudin Abd Shukor

Acceptable Use of Information Technology Policy
Dasar Penggunaan Yang Diterima Pakai Untuk Teknologi Maklumat

1.0 Purpose
1.0 Tujuan

The purpose of this policy is to outline the acceptable use of computers, servers, network equipment, internet facilities and other IT related equipment at UniMAP ICT Center. These rules are in place to protect the employee and UniMAP ICT Center from harm, loss of reputation, misuse and disruption of service. Inappropriate use exposes UniMAP ICT Center and the University to risks including malware attacks, compromise of network systems and services, and legal issues.

Tujuan dasar ini ialah untuk menggariskan penggunaan yang diterima pakai untuk komputer, server, peralatan rangkaian, kemudahan internet dan peralatan lain yang berkaitan dengan IT di Pusat ICT UniMAP. Peraturan-peraturan ini di tempatkan bagi melindungi staf dan Pusat ICT UniMAP dari kemudaratan, kehilangan reputasi, penyalahgunaan dan gangguan perkhidmatan. Penggunaan yang tidak sesuai mendedahkan Pusat ICT UniMAP dan Universiti kepada risiko-risiko termasuk serangan malware, sistem-sistem rangkaian dan perkhidmatan-perkhidmatan dikompromi dan isu-isu perundangan.

2.0 Scope
2.0 Skop

This policy applies to employees, contractors, consultants, temporaries (Staff, Interns), and other workers at UniMAP ICT Center, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by UniMAP ICT Center.

Dasar ini diguna pakai untuk semua staf, kontraktor, konsultan, staf atau pelatih sementara, dan pekerja-pekerja lain di Pusat ICT UniMAP, termasuk semua staf/pegawai yang bergabung dengan pihak ketiga. Dasar ini diguna pakai untuk semua peralatan yang dimiliki atau disewa oleh Pusat ICT UniMAP.

3.0 Policy
3.0 Dasar

3.1 General Use and Ownership
3.1 Penggunaan Am dan Pemilikan

1. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing are the property of UniMAP ICT Center. These systems are to be used for business purposes in serving the interests of the University, and of our uses and stakeholders in the course of normal operations.
1. *Internet / Intranet / sistem-sistem berkaitan Extranet, termasuk tetapi bukan terhad kepada peralatan komputer, perisian, sistem-sistem pengendalian, media storan, akaun-akaun rangkaian yang menyediakan mel elektronik, WWW adalah harta milik Pusat ICT UniMAP. Sistem-sistem ini akan digunakan untuk tujuan-tujuan perniagaan dalam menyampaikan kepentingan Universiti, dan untuk penggunaan universiti dan pemegang-pemegang saham dalam operasi-operasi biasa.*

2. While UniMAP's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the university systems remains the property of UniMAP ICT Center. However, management cannot guarantee the confidentiality of personal information stored on any network device belonging to UniMAP ICT Center. In any case it is discouraged to store personal data of the user that is not related to their work in UniMAP systems.
2. *Walaupun keinginan pengurusan rangkaian UniMAP untuk menyediakan satu tahap privasi yang munasabah, pengguna-pengguna harus sedar bahawa data yang diwujudkan dalam sistem universiti kekal sebagai harta milik Pusat ICT UniMAP. Walau bagaimanapun , pengurusan tidak boleh menjamin kerahsiaan maklumat peribadi yang disimpan di mana-mana peralatan rangkaian kepunyaan Pusat ICT UniMAP. Walau bagaimanapun pengguna adalah tidak digalakkan untuk menyimpan data peribadi yang tidak berkaitan dengan kerja mereka dalam sistem UniMAP.*

3. For security and network maintenance purposes, authorized individuals within UniMAP ICT Center may monitor equipment, systems and network traffic at any time.
3. *Untuk tujuan keselamatan dan penyenggaraan rangkaian, individu-individu yang diberi kebenaran dalam Pusat ICT UniMAP boleh memantau peralatan, sistem-sistem dan trafik rangkaian pada bila-bila masa.*

4. UniMAP ICT Center reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
4. *Pusat ICT UniMAP berhak untuk mengaudit jaringan dan sistem-sistem secara berkala bagi memastikan dasar ini dipatuhi.*

3.2 Security and Proprietary Information
3.2 Maklumat Pemilik dan Keselamatan

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as Highly Restricted, Confidential, Dept Use Only and Unclassified as defined in the Asset Register. Examples of confidential information include but are not limited to: University's strategies, competitor sensitive, instructions from the Government, specification, student information, financials, contracts and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
1. *Antara muka (interface) pengguna untuk maklumat yang dimuatkan di Internet / Intranet / sistem-sistem berkaitan Extranet seharusnya diklasifikasikan sebagai Sangat Terhad, Rahsia, Untuk Kegunaan Jabatan Sahaja dan Tidak Diklasifikasi, seperti yang ditentukan dalam Pendaftaran Aset. Contoh-contoh maklumat rahsia termasuk tetapi tidak dibataskan kepada: Strategi-strategi universiti, maklumat sensitif pesaing, arahan-arahan daripada Kerajaan, spesifikasi, maklumat pelajar, kewangan, kontrak-kontrak dan data kajian. Staf-staf perlu mengambil semua langkah perlu bagi menghalang akses tidak sah kepada maklumat ini.*

2. Postings by employees from an UniMAP ICT Center email address to newsgroups should contain a *disclaimer* stating that the opinions expressed are strictly their own and not necessarily those of UniMAP ICT Center , unless posting is in the course of business duties.
2. *Penghantaran oleh staf-staf dari alamat e-mel Pusat ICT UniMAP ke newsgroups hendaklah mengandungi satu penyataan penafian bahawa pendapat-pendapat yang dinyatakan adalah semata-mata pendapat mereka sendiri dan tidak semestinya Pusat ICT UniMAP, melainkan penghantaran melibatkan tugas-tugas yang diamanahkan.*

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at *10 minutes*, or by logging-off when the host will be unattended.
3. *Semua computer peribadi, komputer riba dan stesen-stesen kerja sepatutnya dijamin dengan screensaver yang dilindungi dengan kata laluan dengan set ciri pengaktifan automatik pada 10 minit, atau dengan logging-off apabila host tidak digunakan.*

4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
4. *Staf-staf perlu berwaspada apabila membuka lampiran e-mel yang diterima dari pengirim tidak dikenali, yang boleh mengandungi virus, e-mel bom atau kod Trojan horse.*

3.3 Unacceptable Use
3.3 Penggunaan Yang Tidak Diterima Pakai

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of UniMAP ICT Center authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UniMAP ICT Center-owned resources.
Company equipment shall not be used for personal benefits/ entertainment especially those pertaining to pornography, gambling, gaming, MP3/4 downloads, YouTube or other media players. Users of the system is prohibited from using UniMAP systems to create, disperse, distribute to any one materials that are religious, race, politically deemed sensitive in Malaysian culture. If they receive any such information/ materials from outside, they shall immediately inform the ICT Director and follow instructions.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Aktiviti-aktiviti berikut adalah, secara amnya, dilarang. staf-staf boleh dikecualikan dari sekatan-sekatan ini semasa menjalankan tanggungjawab-tanggungjawab tugas sah mereka (contoh, staf pengurusan sistem mungkin mempunyai keperluan untuk melumpuhkan akses rangkaian sesuatu host jika host tersebut mengganggu perkhidmatan-perkhidmatan pengeluaran). Di bawah tiada apa jua keadaan sekalipun seseorang staf Pusat ICT UniMAP dibenarkan untuk melibatkan diri dengan apa-apa aktiviti yang tidak dibenarkan di bawah undang-undang setempat, negeri, persekutuan atau antarabangsa ketika menggunakan sumber-sumber yang dimiliki oleh Pusat ICT UniMAP.
Peralatan syarikat tidak akan digunakan untuk faedah peribadi / hiburan terutama yang berkaitan dengan pornografi, perjudian, permainan, MP3 / 4 muat turun, YouTube atau pemain-pemain media lain. Pengguna-pengguna

sistem dilarang daripada menggunakan sistem UniMAP untuk mewujudkan, menyebarkan, mengagihkan mana-mana satu bahan-bahan yang berunsurkan keagamaan, bangsa, secara politik dianggap sensitif dalam budaya Malaysia. Jika mereka menerima mana-mana maklumat / bahan-bahan tersebut dari luar, mereka akan dengan serta-merta memaklumkan Pengarah ICT dan mengikut arahan yang diberi.

Senarai-senarai di bawah tidak bermakna lengkap, tetapi cubaan untuk menyediakan satu rangka kerja bagi aktiviti-aktiviti yang terbahagi kepada kategori penggunaan yang tidak boleh diterima pakai.

3.3.1 System and Network Activities
3.3.1 Aktiviti-aktiviti Sistem dan Rangkaian

The following activities are strictly prohibited, with no exceptions:
Aktiviti-aktiviti berikut dilarang sama sekali, tanpa pengecualian:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UniMAP ICT Center .
1. *Pencabulan hak-hak perseorangan atau organisasi yang dilindungi oleh hak cipta terpelihara, rahsia perdagangan, paten atau harta hak milik intelektual lain, atau undang-undang atau peraturan-peraturan yang serupa dengannya, termasuk, tetapi tidak terhad untuk, pemasangan atau pengagihan perisian cetak rompak atau produk perisian lain yang tidak selayaknya dilesenkan untuk kegunaan Pusat ICT UniMAP.*

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UniMAP ICT Center or the end user does not have an active license is strictly prohibited.
2. *Penyalinan yang tidak diluluskan bahan hak cipta terpelihara termasuk, tetapi tidak dihadkan untuk, pendigitan dan pengagihan gambar-gambar dari majalah-majalah, buku-buku atau lain-lain sumber hak cipta terpelihara, muzik berhak cipta terpelihara, dan pemasangan mana-mana perisian yang berhak cipta terpelihara yang mana Pusat ICT UniMAP atau pengguna akhir tidak mempunyai lesen aktif adalah dilarang sama sekali.*

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. *Pengenalan program-program perosak ke dalam rangkaian atau pelayan (contohnya, virus, worms, Trojan horses, bom e-mail, dan sebagainya.).*

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
4. *Mendedahkan kata laluan akaun anda kepada orang lain atau membenarkan penggunaan akaun anda oleh orang lain. Ini termasuk anggota rumah dan ahli-ahli keluarga lain apabila kerja dilakukan di rumah.*

5. Using an UniMAP ICT Center computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
5. *Menggunakan aset pengkomputeran Pusat ICT UniMAP untuk melibatkan diri secara aktif dalam memperolehi atau menghantar bahan yang termasuk dalam pencabulan gangguan seksual atau undang-undang tempat kerja dalam kuasa setempat pengguna.*

6. Making fraudulent offers of products, items, or services originating from any UniMAP ICT Center account.
6. *Membuat tawaran palsu produk, barang-barang, atau perkhidmatan yang berasal dari mana-mana akaun Pusat ICT UniMAP.*

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, ‘disruption’ includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. *Mengakibatkan pelanggaran keselamatan atau gangguan-gangguan komunikasi rangkaian. Pelanggaran keselamatan termasuk, tetapi tidak dibataskan kepada, mengakses data di mana staf tersebut bukanlah penerima yang dimaksudkan atau logging ke dalam pelayan atau akaun yang tidak dinyatakan secara terbuka sebagai dibenarkan untuk staf tersebut untuk akses, melainkan tugas-tugas ini ialah di dalam skop tugas-tugas biasa. Untuk tujuan seksyen ini, ‘gangguan’*

termasuk, tetapi tidak dibataskan kepada, rangkaian sniffing, pinged floods, packet spoofing, penafian perkhidmatan, dan maklumat penghalaan palsu untuk tujuan-tujuan berniat jahat.

8. Port scanning or security scanning is expressly prohibited unless prior notification to the Head of Networks and MIS is made.
8. *Pengimbasan port atau pengimbasan keselamatan dilarang secara terbuka melainkan pemberitahuan terdahulu dibuat kepada Ketua Unit Rangkaian dan Sistem Maklumat.*

9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. *Melaksanakan sebarang bentuk pemantauan rangkaian yang akan menyekat data yang bukan bertujuan untuk host staf, melainkan aktiviti ini ialah sebahagian daripada kerja / tugas biasa staf tersebut.*

10. Circumventing user authentication or security of any host, network or account without proper justification related to daily work.
10. *Memintasi pengesahan pengguna atau keselamatan sebarang host, rangkaian atau akaun tanpa justifikasi sesuai berkaitan dengan kerja harian.*

11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
11. *Masuk campur dengan atau menafikan perkhidmatan bagi mana-mana pengguna selain daripada host staf (contohnya, penafian serangan servis).*

3.3.2 Email and Communications Activities
3.3.2 Aktiviti-aktiviti E-mel dan Komunikasi-komunikasi

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
1. *Menghantar pesanan e-mel tanpa diminta, termasuk penghantaran "junk mail" atau bahan iklan lain kepada individu yang tidak secara khususnya meminta bahan tersebut (spam e-mel).*

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
2. *Sebarang bentuk gangguan melalui e-mel, telefon atau alat kelui, sama ada melalui bahasa, frekuensi, atau saiz mesej.*

3. Unauthorized use, or forging, of email header information.
3. *Penggunaan tanpa kebenaran, atau pemalsuan, maklumat pengepala e-mel.*

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
4. *Permintaan e-mel untuk mana-mana alamat e-mel lain, selain daripada akaun poster, dengan niat mengganggu atau mengutip balasan-balasan.*

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. *Mencipta atau menghantar surat-surat berantai, Ponzi atau lain-lain jenis skim-skim piramid.*