Information Security Management System
ISO/IEC 27001:2013

RULES AND REGULATIONS FOR THE USE OF ICT FACILITIES

PERATURAN DAN KAEDAH PENGGUNAAN KEMUDAHAN ICT

For PTM Use Only	Version 1.1	Date: 13th Nov 2015
Written By: Asiah Abu Samah Pengerusi Jawatankuasa ISMS	**Verified By:** Nor'Ain bt Mohamed Wakil Pengurusan Keselamatan Maklumat (ISMR)	**Approved By:** Dr David Asirvatham

Revision History

No	Date of Change	Description	Page	Version	Approved By
1.	13 Nov 2015	Merge content with ICT Assets Usage Policy : Clauses in ICT Assets Usage Policy inserted into this document. They are : Clause 1.0 Clause 4.1 Clause 4.5.1- 4.5.10 Clause 4.6.1 – 4.6.2	Throughout dcoument	1.1	Dr David Asirvatham
		Change Document name from Rules and Regulations Regarding ICT Facilities to Rules And Regulations For The Use Of ICT Facilities	Throughout document	1.1	Dr. David Asirvatham

1.0 Purpose

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

2.0 Scope

The rules and regulations apply to :

i) all users of UM's ICT facilities.

ii) all computers and IT devices, including but not limited to computers, laptops, mobile devices, network switches and servers.

However, the scope for ISMS audit and certification only covers PTM staff, interns and its vendor as well as 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

4.1. General Use

UM's ICT facilities are to be used for official purposes in serving the interests of the University, and of our users and stakeholders in the course of normal operations only.

4.2. Access to Facilities

4.2.1. If you connect any device (wired or wireless) to the University network or using any UM's ICT facilities, 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.

4.2.2. 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)/IT Director.

4.2.3. 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.

4.3. Use of Facilities

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.

4.4. You MUST :

4.4.1. obtain written permission from the CIO/IT Director before running any unauthorised services that can lead to security vulnerabilities and can cause connection problems for you and other network users. Unauthorised services, include but not limited to Port scanning, setting up servers, setting up network devices.

4.4.2. be responsible for the use of all ICT resources allocated to you.

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

4.4.4. keep your passwords secure. Do not disclose them to, or allow them to be used by any other person. It is against the rule to give your password to other person(s).

4.4.5. 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 by the authorities.

4.4.6. ensure your computer have up-to-date anti-virus software that updates automatically from a trusted software vendor. PTM has the right to disconnect your device(s) from the network if your device becomes infected with viruses, malware or if it displays suspicious network activity. For more details, refer to UM Malware Policy.

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

4.5. Unacceptable Use

The following activities are, in general, prohibited. UM authorised staff 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).

4.5.1. Under no circumstances is UM ICT Facilities' users authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UM-owned resources.

4.5.2. UM's ICT Facilities shall not be used for personal benefits/entertainment especially but not limited to those pertaining to pornography, gambling, gaming, MP3/4 downloads, video streaming or other media players.

4.5.3. Users of the system are prohibited from using UM systems to create, disperse, distribute any material that are religious, race, politically deemed sensitive in Malaysian culture. If they receive such information/ materials from outside, they shall immediately inform PTM Director.

4.5.4. 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 UM

4.5.5. 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 UM or the end user does not have an active license is strictly prohibited.

4.5.6. 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.

4.5.7. Using UM computing assets 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.

4.5.8. Making fraudulent offers of products, items, or services originating from any UM official identity/account.

4.5.9. Any activity that involves interception of data which is not part of the employee's normal job/duty.

4.5.10. Circumventing user authentication or security of any host, network or account without proper justification related to daily work.

4.5.11. Attempting 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.

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

4.5.13. Making 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.

4.5.14. Altering or destroying data belongs to other users.

4.5.15. Using 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.

4.5.16. Connecting 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/IT Director.

4.5.17. Using any file-sharing software or participate in Peer-to-Peer (P2P) file-sharing networks unless prior written permission is obtained from the CIO/IT Director. If you are found to have P2P software running on your computer you will be subject to appropriate action by the University.

4.5.18. Illegal Port scanning or security scanning on UM ICT facilities is strictly prohibited. Scans are considered dangerous and unethical actions.

4.5.19. Using campus ICT resources to disrupt or threaten the safety of others

4.5.20. Any activity affecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the person is not an intended recipient or logging into a server or account that the person is not expressly authorized to access, unless these duties are within the scope of authorised duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, interfering with or denying service to other users (eg. denial of service), and forged routing information for malicious purposes.

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

4.5.22 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.

4.5.23 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. Monitoring and securing the network

4.6.1. For security and network maintenance purposes, authorized individuals within PTM may monitor equipment, systems and network traffic at any time.

4.6.2. PTM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.6.3. 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.

4.6.4. 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.

4.6.5. 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.

4.6.6. 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.