Information Security Management System

MS ISO/IEC 27001:2007

REMOVAL OF MEDIA POLICY

DASAR PEMINDAHAN MEDIA

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
Pn. Ummi Naiemah Saraih ISMR	Pn. Rohazna Wahab Deputy Director ICT	En. Nasrudin Abd. Shukor Director ICT Division

For Dept Use Only

Date: 15th Oct 2012 **Version 1.0**

Revision History

No	Date of Change	Description	Page	Version	Approved By

REMOVAL OF MEDIA POLICY
DASAR PEMINDAHAN MEDIA

1.0 POLICY

1.0 DASAR

Increasing amounts of electronic data are being transmitted and stored on computer systems and electronic media by virtually every person conducting business for UniMAP ICT Centre. Some of that data contains sensitive information, including student records, personnel records, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of, that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within UniMAP ICT Centre, including contractors and vendors with access to UniMAP ICT Centre systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal. Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as usb drives.

Bilangan data elektronik yang disiarkan, disampaikan dan disimpan di sistem-sistem komputer dan media elektronik oleh hampir setiap individu yang menjalankan perniagaan untuk Pusat ICT UniMAP bertambah. Sebahagian daripada data tersebut mengandungi maklumat sensitif, termasuk rekod-rekod pelajar, rekod-rekod kakitangan, data kewangan , dan maklumat kesihatan yang dilindungi. Jika maklumat di sistem-sistem ini tidak dipindahkan dengan betul sebelum peralatan dibuang atau dimusnahkan, maklumat tersebut boleh di akses dan dilihat oleh individu-individu yang tidak diluluskan. Oleh itu, semua pengguna sistem komputer dalam Bahagian ICT UniMAP, termasuk kontraktor-kontraktor dan vendor-vendor dengan akses kepada sistem-sistem Bahagian ICT UniMAP, bertanggungjawab untuk mengambil langkah-langkah bersesuaian, seperti yang digariskan di bawah untuk memastikan bahawa semua komputer-komputer dan media elektronik di sanitasi dengan betul sebelum pelupusan. Media Elektronik didefinisikan sebagai mana-mana peranti storan elektronik yang digunakan untuk merekod maklumat, termasuk, tetapi tidak terhad kepada cakera keras, pita-pita magnetik, cakera-cakera padat, pita-pita video, pita-pita audio , dan alat-alat simpanan mudah alih seperti pemacu usb.

2.0 RATIONALE

2.0 RASIONAL

The purpose of this policy is to establish a standard for the proper disposal of electronic media containing sensitive data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

Tujuan dasar ini ialah untuk mewujudkan satu standard pelupusan bersesuaian untuk media elektronik yang mengandungi data sensitif. Prosedur-prosedur pelupusan yang digunakan akan bergantung kepada jenis dan kecenderungan media tersebut. Media elektronik mungkin dijadualkan untuk kegunaan semula, pembaikan, penggantian, atau penyingkiran daripada perkhidmatan kerana beberapa sebab dan dihapuskan dalam pelbagai cara seperti yang diterangkan di bawah.

3.0 PROCEDURES

3.0 PROSEDUR

Standards

Standards

Electronic Media is defined as any storage that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, video tapes, audio tapes, and removable storage such as USB drives, SD Cards, Micro SD amongst others.

All UniMAP ICT Centre electronic media should undergo a complete format before the media, or the system containing the media, is disposed or transferred to another external agency such as service provider for repairs. If a complete overwrite of the media is not an option, then the media should be destroyed so that the information is not recoverable without unreasonable time or cost. This standard is necessary to protect all university information, and to comply with software license agreements.

Confidential Information is important and sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Some examples of confidential information are system passwords or

encryption keys, financial records, proprietary information, human resource or personnel records, student records, and patient records. All media that contains confidential information should be overwritten a minimum of three times with software designed to "zero out" media tracks or destroyed. Other confidential information may be defined by federal or state laws such as Personal Data Protection Act Malaysia (PDPA) 2010. Examples of solutions for overwriting media are included below.

Note: All Server hard drives are drilled for destruction during disposal. Removing the partition information from the media, such as using FDisk, is not sufficient. Reinstalling the operating system, without first completing a full media overwrite is not sufficient. Removing the media and disposing of it in any way that does not render it difficult to recover is not sufficient. Using a magnetic degaussing tool is not reliable for every form of media, e.g. modern hard disks may not be completely erased with most degaussing tools.

Software programs that can be used to overwrite media include:

- WipeDrive Pro
- File Shredder
- Eraser
- KillDisk

Media Elektronik didefinisikan sebagai mana-mana penstoran yang digunakan untuk merekod maklumat, termasuk, tetapi tidak terhad kepada cakera-cakera keras, pita-pita magnetik, cakera-cakera padat, pita-pita video, pita-pita audio, dan storan mudah alih seperti USB Drives, Kad-kad SD, Mikro SD antara lainnya.

Semua media elektronik Pusat ICT UniMAP seharusnya menjalani satu format lengkap sebelum media, atau sistem yang mengandungi media, dilupuskan atau dipindahkan ke agensi luar yang lain seperti penyedia perkhidmatan untuk dibaiki. Jika tulis ganti media yang lengkap bukan satu pilihan, maka media tersebut haruslah dimusnahkan supaya maklumat tidak boleh diperolehi semula tanpa masa atau kos yang tidak munasabah. Standard ini perlu untuk melindungi kesemua maklumat universiti, dan mematuhi perjanjian-perjanjian lesen perisian.

Maklumat Rahsia ialah bahan yang sensitif dan penting. Maklumat yang dikategorikan sebagaisulit atau juga sensitif mesti disekat kepada mereka yang hanya mempunyai keperluan urusan sah untuk akses. Beberapa contoh maklumat rahsia ialah kata-kata laluan sistem atau kunci-kunci enkripsi, rekod-rekod kewangan, maklumat pemilik,

rekod-rekod sumber manusia atau kakitangan, rekod-rekod pelajar , dan rekod-rekod pesakit. Semua media yang mengandungi maklumat sulit seharusnya ditulis ganti sekurang-kurangnya tiga kali dengan perisian yang direka untuk "sifar keluar" jejak media atau dimusnahkan. Maklumat sulit lain boleh dijelaskan oleh undang-undang negeri atau pusat seperti Personal Data Protection Act Malaysia (PDPA) 2010. Contoh-contoh penyelesaian untuk tulis ganti media termasuk di bawah.

Nota: *Semua Server hard drives dimusnahkan secara digerudisemasa pelupusan. Memindahkanmaklumat sekatan dari media, seperti menggunakan FDisk, tidak mencukupi. Memasang semula sistem pengendalian, tanpa terlebih dahulu menyiapkan satu media tulis ganti lengkap tidak mencukupi. Memindahkan media dan menghapuskannya dalam apa jua cara yang tidak menjadinya sukar untuk diperolehi semula tidak mencukupi. Menggunakan alat degaussing magnetik tidak boleh dipercayai untuk setiap bentuk media, misalnya cakera-cakera keras moden tidak boleh sepenuhnya dipadamkan dengan kebanyakan alat-alat degaussing.*

Program-program perisian yang boleh digunakan untuk tulis ganti media termasuk:

- *WipeDrive Pro*
- *File Shredder*
- *Eraser*
- *KillDisk*