Information Security Management System MS ISO/IEC 27001:2007

ACCESS CONTROL POLICY

DASAR KAWALAN AKSES

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
Pn. Ummi Naiemah Saraih	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	Pembetulan approval bagi akses ke SVN	3	1.0	Nasrudin Abd Shukor
2	22 Mac 2013	GENERAL POLICY/DASAR AM 3.0: English – add 'network cable' and 'all visitors should get the network cables from ICT Administration Office' Bahasa Melayu – penambahan 'kabel rangkaian' dan 'Pelawat-pelawat boleh mendapatkan kabel rangkaian daripada pihak pentadbiran ICT'	4	1.0	Nasrudin Abd Shukor

1.0 Purpose
1.0 Tujuan

The purpose of this policy is to establish a standard for the management of all access through the internet/ intranet into UniMAP ICT Center's systems, files, folders and its networks.

Tujuan dasar ini ialah untuk mewujudkan satu piawaian bagi pengurusan semua akses melalui internet / intranet ke dalam sistem-sistem, fail-fail, folder-folder dan rangkaian Pusat ICT UniMAP.

2.0 Scope
2.0 Skop

The policy applies to all UniMAP ICT Center staff logging into UniMAP's servers using the LAN or the internet. This policy also covers physical access by visitors/ students and vendors into UniMAP ICT Center premises. The Data center and the DR site in Pauh Campus may have additional controls in place as deemed appropriate and approved by the management.

Dasar diguna pakai atas semua staf Pusat ICT UniMAP yang log ke dalam pelayan UniMAP menggunakan LAN atau internet. Dasar ini juga meliputi akses fizikal oleh pelawat / pelajar dan pembekal ke dalam premis-premis Pusat ICT UniMAP. Pusat data dan tapak Pemulihan Bencana di kampus Pauh mungkin mempunyai kawalan-kawalan tambahan di tempatkan seperti yang dianggap sesuai dan diluluskan oleh pengurusan.

3.0 General Policy
3.0 Dasar Am

3.1 All critical or sensitive systems must be isolated logically.
3.1 Semua sistem-sistem kritikal atau sensitif mesti diasingkan mengikut logik.

3.2 All logging mechanism to the domain, in UniMAP ICT Center must be synchronized.
3.2 Semua mekanisma logging ke domain, dalam Pusat ICT UniMAP mesti diselaraskan.

3.3 The logging mechanism must be customized to have sufficient integrity and information to allow investigation and reconstruction.
3.3 Mekanisma logging mesti dibuat mengikut tempahan yang sesuai untuk mempunyai integriti yang mencukupi dan maklumat untuk membenarkan siasatan dan pembinaan semula.

3.4 Only authorized users (IT administrator) is allowed to exam the audit dan fault logs.

3.4 Hanya pengguna yang diberi kebenaran (Pentadbir IT) dibenarkan untuk memeriksa audit dan kesalahan log.

3.5 All *event log*s must undergo monthly review to detect possible subtle attacks or suspicious events or whenever there is a suspicion.

3.5 Semua log peristiwa mesti menjalani kajian semula secara bulanan untuk mengesan kemungkinan serangan-serangan yang tidak ketara atau kejadian yang mencurigakan atau bila-bila masa terdapat kesangsian.

3.6 All access to software/ applications being developed in applications department under MIS will be controlled by the SVN tool. The access levels will be granted by the Head of MIS based on Segregation of Duty document.

3.6 Kawalan capaian kepada perisian / aplikasi-aplikasi yang dibangunkan dalam jabatan aplikasi-aplikasi di bawah MIS akan dikawal oleh alat SVN. Aras capaian akan diberi oleh Ketua Bahagian MIS berdasarkan dokumen Pengkelasan Tugas

3.7 All testing will be carried out on an isolated test server to prevent any damage to their existing equipment.

3.7 Semua ujian akan dijalankan di server ujian terpencil untuk menghalang sebarang kerosakan bagi peralatan yang sedia ada.

3.8 Employee are only given the minimum amount of access control to UniMAP ICT Center Information System, as required to complete his/her daily task. (Access Privileges). These privileges are determined by the department head and approved by the ICT Director, the administrator informed to allocate access.

3.8 Staf hanya diberi jumlah kawalan akses yang minimum kepada Sistem Maklumat Pusat ICT UniMAP, seperti yang dikehendaki bagi melengkapkan / tugas seharian mereka. (Keistimewaan Akses). Keistimewaan ini ditentukan oleh ketua bahagian dan diluluskan oleh Pengarah ICT, pentadbir dimaklumkan untuk memperuntukkan akses.

3.9 Upon employee resignation/ termination or task completion, employee access control to the relevant UniMAP ICT Center Information System must be removed or suspended within 24hours. This will be accomplished by using a checklist and then HR department is to be notified.

3.9 Sebaik sahaja staf meletakkan jawatan / diberhentikan atau tamat tugas, kawalan akses staf kepada Sistem Maklumat Pusat ICT UniMAP berkenaan mesti dibatalkan atau digantung dalam masa 24 jam. Ini akan dilaksanakan dengan menggunakan senarai semakan dan kemudian Jabatan Sumber Manusia akan dimaklumkan.

3.10 Any documents or information access given to 3rd party will only be carried out to fulfill business functions and immediate needs;

3.10 Sebarang akses dokumen atau maklumat diberikan kepada pihak ketiga hanya akan dijalankan untuk memenuhi fungsi perniagaan dan keperluan segera;

3.11 Visitors shall not be allowed to plug network cable into any ports that are not authorized by Network department. All visitors should get the network cables from ICT Administration Office.

3.11 Pelawat-pelawat tidak dibenarkan untuk memasang sebarang kabel rangkaian ke dalam mana-mana port yang tidak dibenarkan oleh Bahagian Rangkaian.Pelawat-pelawat boleh mendapatkan kabel rangkaian daripada pihak pentadbiran ICT.

3.12 A Role Based Access Control (RBAC) system is established. This includes access privileges and access rights.

3.12 Sistem Kawalan Akses Berdasarkan Peranan (RBAC) ditubuhkan. Ini termasuk keistimewaan akses dan hak akses.

4.0 User Access Policy
4.0 Dasar Kawalan Pengguna

4.1 All user who require access to UniMAP ICT Center computer equipment must submit a request through their HOD. The HOD will e-mail the network/ MIS of UniMAP head to grant access.

4.1 Semua pengguna yang memerlukan akses kepada peralatan komputer Pusat ICT UniMAP mesti mengemukakan satu permintaan melalui Ketua Jabatan mereka. Ketua Jabatan akan menghantar e-mel kepada Ketua Bahagian Rangkaian / Ketua MIS UniMAP untuk membenarkan akses.

4.2 User access will only be approved by the MIS/ Network Head.

4.2 Akses pengguna hanya akan diluluskan oleh Ketua Bahagian MIS/Rangkaian.

4.3 Only authorized personnel is able to grant access to the relevant computer equipments base on the approved access request.

4.3 Hanya staf yang diberi kebenaran dibolehkan untuk memberi akses bagi peralatan komputer berkenaan berdasarkan permintaan akses yang diluluskan.

4.5 All third party access to systems shall be supervised by the relevant person who is tasked with the responsibility of the visitor(s).

4.5 Semua akses pihak ketiga kepada sistem-sistem akan diawasi oleh individu berkenaan yang ditugaskan dengan tanggungjawab pelawat.

4.6 Only the MIS head or his/her authorized personnel is able to revoke access from the relevant computer equipments based on the approved access revocation request in the HR termination checklist.

4.6 Hanya ketua MIS atau / staf yang diberi kebenaran oleh beliau yang mampu membatalkan akses dari peralatan-peralatan komputer berkenaan berdasarkan permintaan pembatalan akses yang diluluskan dalam senarai semakan penamatan sumber manusia.

4.7 User access rights must be subjected to periodic reviewed. (At least once a year)

4.7 Hak-hak akses pengguna mesti dikaji semula secara berkala. (Sekurang-kurangnya sekali setahun)

4.8 All users must have a unique identification (username) and password that is alphanumeric with minimum of 6 characters in order to access UniMAP ICT Division computer equipment or networks.

4.8 Semua pengguna mesti mempunyai satu pengenalpastian unik (nama pengguna) dan kata laluan yang berabjad angka dengan minimum 6 karakter untuk mengakses peralatan komputer atau rangkaian Pusat ICT UniMAP.

4.9 A network connect must be disconnect after 10 minutes of inactivity on the Connection, 3 months freeze of account if not used and 6 months automatic deletion.

4.9 Sambungan rangkaian mesti diputuskan selepas 10 minit ketidakaktifan di sambungan, pembekuan akaun selama 3 bulan jika tidak digunakan dan pemotongan automatik untuk 6 bulan.

4.10 User access names will be maintained by MIS division.

4.10 Nama-nama akses pengguna akan diselenggara oleh Bahagian MIS.

4.11 Access to the database and critical servers (Root Access/ Super-User Password) must be only with the head of Data centre, MIS, Networks and for their own servers and systems. They shall not be allowed access to other systems that are not in their RBAC list. Only the ICT Director will maintain a full access password list kept in a safe and lock.

4.11 Akses bagi pangkalan data dan pelayan kritikal (Root Access / Kata Laluan Super-User) mesti hanya dengan ketua Pusat Data, MIS, Rangkaian dan untuk pelayan dan sistem mereka sendiri. Mereka tidak akan dibenarkan akses bagi lain-lain sistem yang tidak tersenarai dalam RBAC mereka. Hanya Pengarah ICT akan mempunyai senarai penuh kata laluan akses yang disimpan di dalam sebuah peti besi/unit simpanan/bilik berkunci.

5.0 Remote Access Policy

5.0 Dasar Akses Jarak Jauh

5.1 Remote access to organization network is governed by VPN client and must be renewed every half yearly.

5.1 Akses jarak jauh kepada rangkaian organisasi dikawal oleh client VPN dan mesti diperbaharui setiap setengah tahun.

5.2 Remote access to organization network must logged.

5.2 Akses jarak jauh kepada rangkaian organisasi mesti di log.

5.3 Remote access must be kept to a bare minimum as practical. The company discourages the use of remote access by junior level staff.

5.3 Akses jarak jauh mesti dikekalkan pada tahap praktikal seminimum mungkin. Organisasi tidak menggalakkan penggunaan akses jarak jauh oleh staf peringkat rendah.

6.0 Network Segregation Policy

6.0 Dasar Pengasingan Rangkaian

6.1 The organization network must be segmented based on the organization Unit functionality.

6.1 Rangkaian organisasi mesti dibahagi berdasarkan fungsi Unit di dalam organisasi.

6.2 Access to critical network segment must be restricted. Users are only given access to relevant network segment that are required to complete their daily job or assigned task.

6.2 Akses untuk segmen rangkaian kritikal mesti dihadkan. Pengguna-pengguna hanya diberikan akses untuk segmen rangkaian yang dikehendaki bagi melengkapkan kerja harian mereka atau tugasan yang diberi.

7.0 Physical Access Control

7.0 Kawalan Akses Fizikal

7.1 All access to sensitive areas within ICT division will be controlled. Data center, Help Desk room, Admin office, MIS and Network office, and other areas identified by Red Label/ signage outside the door will be controlled by Card access system or other equally good method.

7.1 Kesemua akses kepada kawasan sensitif dalam Pusat ICT akan dikawal. Pusat data, bilik Help Desk, pejabat Pentadbiran, pejabat MIS dan Rangkaian, serta kawasan lain yang dikenal pasti oleh Red Label / papan tanda luar pintu akan dikawal oleh sistem akses kad atau kaedah lain yang sama baik.

7.2 All staff/temporary, students, and vendor working in ICT division shall carry their name tags clearly displayed on their person.

7.2 Semua staf/sementara, pelajar-pelajar, pembekal yang bekerja dalam Pusat ICT akan membawa tag-tag nama mereka yang dipamerkan dengan jelas.

7.3 Warning Signage shall be displayed in all restricted areas within ICT division.

7.3 Papan Tanda Amaran akan dipamerkan di semua kawasan-kawasan terhad dalam Pusat ICT.

7.4 CCTV cameras shall be placed in sensitive areas covering these doors and access points.

7.4 Kamera CCTV akan ditempatkan dikawasan sensitif bagi melindungi pintu-pintu dan kawasan akses.

7.5 All cleaning staff shall be vetted by the Procurement department with proper NDA signed with the service provider. Such cleaning staff shall have ID badges displayed on self at all times.

7.5 Semua staf pembersihan akan diperiksa oleh jabatan Perolehan dengan Perjanjian Ketakdedahan bersesuaian yang ditandatangani dengan penyedia perkhidmatan. Staf pembersihan sedemikian akan mempunyai lencana-lencana ID yang dipakai dan dipamerkan sepanjang masa.

7.6 There will be an hourly patrol of security guards after office hours around the ICT division building.

7.6 Akan ada rondaan setiap satu jam yang dilakukan oleh pengawal-pengawal keselamatan selepas waktu pejabat sekitar bangunan Pusat ICT.

7.8 All vehicles passing out of ICT division at night will be logged in the guard outpost at the gate with license plate details.

7.8 Semua kenderaan yang lalu keluar daripada Pusat ICT pada waktu malam akan di log masuk di pintu pagar pengawal dengan butiran plat lesen.

7.9 Master Keys and room access keys will be tightly controlled by the admin department of ICT Division.

7.9 Kunci-kunci Induk dan kunci-kunci akses bilik akan dikawal dengan rapi oleh Bahagian pentadbiran Pusat ICT.