Information Security Management System MS ISO/IEC 27001:2007

SERVER SECURITY POLICY

DASAR KESELAMATAN SERVER

UNIVERSITI MALAYSIA PERLIS

Writen By:	Verified By:	Approved By:
En. Mohd Nasri Bin Mat Isa IT Officer	Pn. Rohazna Wahab Deputy Director ICT Centre	En. Nasrudin Abd. Shukor Director ICT Centre ISMR

For Dept Use Only

Date: 25th July 2013 **Version 1.1**

Revision History

No	Date of Change	Description	Page	Version	Approved By
1	25/07/2013	Amendment to item no 3.1 : ▪ Owner of all internal servers include the System Administrator ▪ Reference changed to Asset Register and System Administrator and List of Servers Password Document	3	1.1	En. Nasrudin Abd. Shukor
2	25/07/2013	Amendment to item no 3.9 : ▪ All logs have to logged according to Incident Management Procedures ▪ Audit Logs will be reviewed at least once in 6 months	4	1.1	En. Nasrudin Abd. Shukor
3	25/07/2013	New policy added item no 3.12 : ▪ Server Rack facilities to the Other Departments / Parties	5	1.1	En. Nasrudin Abd. Shukor
4	25/07/2013	Amendment to item no 4.6 : ▪ Each operational group must establish a process for changing the configuration guides, which includes review and approval by Head of Department.	6	1.1	En. Nasrudin Abd. Shukor
5	25/07/2013	Amendment to item no 4.6 : ▪ Any incident is managed based on Incident Management Procedures ▪ Security-related events will be reported to the ISMR / ISMS Coordinator	8	1.1	En. Nasrudin Abd. Shukor

6	25/07/2013	Amendment to item no 4.7 : ▪ Changed BU head to Head of Department ▪ System Audits will be performed on a regular basis and records maintained by operational group or System Administrator. ▪ Operational group or System Administrator will submit the findings to the Head of Division for management and decision action.	9	1.1	En. Nasrudin Abd. Shukor

1.0 Purpose
1.0 Tujuan

The purpose of this policy is to establish a standard on the configuration of internal server equipment that is owned or operated by UniMAP ICT Center.

Tujuan dasar ini ialah untuk mewujudkan satu piawaian atas konfigurasi peralatan pelayan dalaman yang dimiliki atau dikendalikan oleh Pusat ICT UniMAP.

2.0 Scope
2.0 Skop

This policy applies to server equipment owned or operated by UniMAP ICT Center, and to servers registered under any UniMAP ICT Center sites-owned internal network domain.

Dasar ini digunapakai atas peralatan pelayan yang dimiliki atau dikendalikan oleh Pusat ICT UniMAP, dan untuk pelayan yang didaftarkan di mana-mana tempat yang dimiliki oleh Pusat ICT UniMAP serta mempunyai 'domain' rangkaian dalaman.

3.0 Policy
3.0 Dasar

3.1 All internal servers including databases deployed at UniMAP ICT Center must be owned by an operational group or System Administrator that is responsible for system administration. (See Asset Register and System Administrator and List of Servers Password Document)

3.1 Semua pelayan dalaman termasuk pangkalan data yang digunakan di Pusat ICT UniMAP mesti dimiliki oleh satu bahagian operasi atau pentadbir sistem yang bertanggungjawab untuk pentadbiran sistem. (Lihat Daftar Aset dan Dokumen Senarai Pentadbir dan Kata Laluan Pelayan)

3.2 Servers must be registered within the Asset Register List. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) Person In Charge and location, and a backup contact PIC
- Hardware and Operating System/Version
- Main functions and applications, if applicable

3.2 Sekurang-kurangnya maklumat berikut diperlukan bagi mengenalpasti pegawai bertanggungjawab yang boleh dihubungi.

- *Kakitangan bertugas serta kakitangan bantuan untuk dihubungi berkaitan pelayan dan lokasi ,*
- *Perkakasan dan Sistem Pengendalian / Versi*
- *Fungsi-fungsi utama dan aplikasi terlibat , jika berkenaan*

3.3 Information in the asset register must be kept up-to-date.

3.3 Maklumat di dalam daftar Aset mestilah sentiasa dikemaskini

3.4 Access to services must be logged and/or protected through access-control methods governed by access control policy.

3.4 Akses kepada perkhidmatan mestilah dicatatkan dan / atau dilindungi melalui kaedah-kaedah kawalan akses yang ditentukan oleh dasar kawalan akses.

3.5 The server must be sufficiently hardened, conforming to standard security practice and guidelines.

3.5 Pelayan mestilah diperkukuhkan sebaiknya, sebagai mematuhi piawaian dan garis panduan mengikut amalan keselamatan

3.6 Always use standard security principles of least required privilege to perform a function.

3.6 Sentiasa mengamalkan prinsip piawaian amalan keselamatan, sekurang -kurangnya memerlukan keutamaan akses untuk menjalankan sesuatu fungsi.

3.7 Remote access must be performed over secure channels (VPN Client).

3.7 Akses jarak jauh hendaklah dilakukan melalui saluran-saluran yang selamat, sebagai contoh menggunakan (VPN Client)

3.8 Servers should be physically located in an access-controlled environment that restricts unauthorized entry.

3.8 Pelayan seharusnya ditempatkan secara fizikal di persekitaran yang mempunyai kawalan akses serta menghadkan akses tanpa kebenaran.

3.9 All security-related events on critical or sensitive systems must be logged according to Security Incident Management Procedures and reviewed at least once in 6 months. (Audit Logs)

3.9 Semua kejadian berkaitan keselamatan di sistem-sistem kritikal atau sensitif mesti di logkan melalui Prosidur Pengurusan Insiden Keselamatan dan disemak semula sekurang-kurangnya sekali dalam setiap 6 bulan. (Log-log Audit)

3.10 Servers must be installed with host-based performance and health check monitoring services.

3.10 Pelayan mesti dipasang dengan prestasi host-based dan perkhidmatan pemantauan keadaan/kondisi.

3.11 Servers must be configured with centralized UniMAP's NTP Server for time or clock synchronization.

3.11 Penyelarasan masa pelayan mestilah menggunakan Pelayan NTP berpusat UniMAP.

3.12 Server Rack facilities to the Other Departments / Parties

- Data Center can receive at his discretion and university requirement for any server to be placed in the server rack provided by UniMAP ICT's Data Centre after a review and approval of the Head of Department and ICT Director.
- The Data Centre is only providing server rack only, by the technical management, risk management and security incident is under that departments or parties own risk.
- Asset owned by other Departments or Parties are not asset of UniMAP ICT's Data Centre
- Any request to other facilities by the other Department / Parties such as backup & restoration, web application firewall and basic maintenance on the server is at the discretion and approval of the Head of Department and ICT Director also depending on the availability of existing resources of data centre facilities.

3.12 Kemudahan Rak Pelayan kepada Jabatan / Pihak Lain

- *Pusat Data boleh menerima diatas budi bicara dan keperluan universiti terhadap sebarang pelayan atau peralatan untuk ditempatkan didalam rak pelayan Pusat Data ICT UniMAP setelah mendapat semakan dan kelulusan Ketua Bahagian dan Pengarah ICT.*
- *Pihak Pusat Data hanya menyediakan kemudahan rak pelayan sahaja, oleh itu pengurusan teknikal, pengurusan risiko dan insiden keselamatan adalah dibawah tanggungjawab sendiri.*
- *Aset Jabatan / Pihak Lain adalah bukan asset Pusat Data ICT UniMAP*
- *Sebarang permohonan kepada kemudahan lain oleh Jabatan / Pihak Lain seperti kemudahan backup & restoration, web application firewall dan penyelenggaraan asas pelayan adalah diatas budi bicara dan kelulusan Ketua Bahagian dan Pengarah ICT serta bergantung kepada kesediaan sumber – sumber Pusat Data yang sedia ada.*

4.0 Procedure

4.0 Prosedur

4.1 Do not use administrative/root access when non-privileged account will do. Root access passwords must be under the control by ICT Director, head of division of Data Center or Head of Operation, Server and Email only. This access password must be frequently changed.

4.1 Penggunaan akses pentadbir/'root' adalah dilarang apabila penggunaan akaun tidak berkeutamaan (akaun pengguna)sudah memadai. Kata laluan akses pentadbir/'root' mestilah di bawah kawalan Pengarah ICT, Ketua Bahagian Pusat Data atau Ketua Unit Operasi, Pelayan dan Emel sahaja. Kata laluan untuk pentadbir/'root' mestilah sentiasa ditukar.

4.2 Services and applications that will not be used must be disabled where practical.

4.2 Perkhidmatan dan aplikasi yang tidak akan digunakan mesti dimansuhkan jika perlu.

4.3 The most recent security patches must be installed on the system as soon as practical, unless immediate application would interfere with business requirements. Follow OS/ application vendor's advice.

4.3 Penambahbaikan keselamatan yang terbaru hendaklah dipasangkan pada sistem apabila perlu, melainkan jika pemasangan segera akan mengganggu keperluan operasi sistem. Sila ikuti nasihat vendor OS/aplikasi.

4.4 Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the ICT director. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Head of Department.

- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

4.4 Panduan konfigurasi pelayan yang diluluskan mesti ditubuhkan dan diselenggara oleh kumpulan operasi masing-masing, berdasarkan keperluan universiti dan diluluskan oleh Pengarah ICT. Kumpulan-kumpulan operasi harus memantau pematuhan konfigurasi dan

melaksanakan dasar pengecualian yang disesuaikan kepada persekitaran mereka. Setiap kumpulan operasi mesti mewujudkan satu proses untuk mengubah panduan konfigurasi, yang termasuk semakan dan kelulusan oleh Ketua Bahagian.

- *Maklumat dalam sistem pengurusan perniagaan korporat mesti dikemas kini dan terkini.*
- *Perubahan konfigurasi untuk pelayan pengeluaran mestilah mengikut prosedur-prosedur pengurusan perubahan bersesuaian.*

4.5 General Configuration Guidelines
4.5 Garis-garis panduan Konfigurasi Am

- Operating System configuration should be in accordance with approved guidelines as per manufacturer guidelines. Default settings must be removed and re-configured.
- *Konfigurasi Sistem Pengendalian sepatutnya sejajar dengan garis-garis panduan yang diluluskan mengikut garis-garis panduan pengeluar. Default Settings mesti dibuang dan dikonfigurasi semula.*

- Services and applications that will not be used must be disabled where practical.
- *Perkhidmatan dan aplikasi yang tidak akan digunakan mesti dimansuhkan jika perlu.*

- Access to services should be logged and/or protected through access control methods such as TCP Wrappers, if possible.
- *Akses kepada perkhidmatan-perkhidmatan seharusnya di log dan / atau dilindungi melalui kaedah-kaedah kawalan akses seperti TCP Wrappers, jika perlu.*

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- *Penambahbaikan keselamatan yang terbaru hendaklah dipasang pada sistem apabila perlu, melainkan jika pemasangan segera akan mengganggu keperluan operasi sistem.*

- Always use standard security principles of least required access to perform a function.
- *Selalu menggunakan prinsip-prinsip keselamatan piawaian yang paling kurang memerlukan akses untuk melakukan fungsi.*

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- *Jika satu kaedah untuk sambungan saluran selamat boleh didapati (misalnya., technically feasible), akses istimewa mesti dilakukan atas saluran-saluran selamat, (misalnya, sambungan rangkaian enkripsi menggunakan SSH atau IPSec).*

- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- *Pelayan adalah dilarang secara khusus daripada beroperasi dari kawasan-kawasan petak tidak terkawal.*

4.6 Monitoring

4.6 Pemantauan/Pengawasan

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 2 month.
- *Semua kejadian berkaitan keselamatan pada sistem kritikal atau sensitif mesti di log dan jejak audit seperti berikut:*
  - *Semua log-log berkaitan keselamatan akan disimpan online untuk sekurang-kurangnya 2 bulan.*

- Security-related events will be reported to the security committee/ ISMR, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host
  - Any incident is managed based on Incident Management Procedures
- *Kejadian-kejadian berkaitan keselamatan akan dilaporkan kepada jawatankuasa keselamatan / ISMR, yang akan mengkaji semula log-log dan laporan kejadian-kejadian kepada pengurusan IT. Tindakan pembetulan akan ditetapkan seperti yang diperlukan. Kejadian-kejadian berkaitan keselamatan termasuk, tetapi tidak dibataskan kepada:*

- *Ancaman-ancaman Port-scan*
- *Bukti akses yang tidak dibenarkan kepada akaun-akaun istimewa*
- *Peristiwa-peristiwa janggal yang tidak berkaitan dengan aplikasi-aplikasi spesifik di host*
- *Sebarang insiden adalah diuruskan berdasarkan prosidur pengurusan insiden*

4.7 Compliance
4.7 Pematuhan

- System Audits will be performed on a regular basis and records maintained by operational group or System Administrator.
- Operational group or System Administrator will submit the findings to the Head of Division for management and decision action.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

- *Audit-audit sistem akan kerap dilakukan dan rekod-rekod diselenggarakan oleh kumpulan operasi atau pentadbir sistem.*
- *Kumpulan operasi atau pentadbir sistem akan mengemukakan penemuan-penemuan kepada ketua Bahagian untuk pengurusan dan keputusan tindakan selanjutnya.*
- *Setiap usaha akan dibuat untuk mencegah audit dari menyebabkan kegagalan-kegagalan atau gangguan-gangguan operasi.*

4.8 Enforcement
4.8 Penguatkuasaan

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- *Mana-mana kakitangan yang didapati telah melanggar dasar ini boleh tertakluk kepada tindakan disiplin, sehingga dan termasuk penamatan perkhidmatan.*