POLISI KESELAMATAN OPERASI IT

Tarikh Kuatkuasa	**21 Feb 2005**	Pindaan		Diluluskan Oleh	Naib Canselor UNISEL

14.1 Tujuan Polisi

Tujuan polisi adalah untuk memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer.

14.2 Skop Polisi

Merangkumi pelbagai aspek perkakasan dan perisian seperti sistem komputer, data-data pinggiran, sistem pengoperasian, pangkalan data dan sistem aplikasi.

14.3 Keselamatan Sistem Komputer/Server

14.3.1 Kawalan Capaian Fizikal

i. Kawalan terhadap individu/staf yang masuk ke Bilik Komputer dan juga kawalan akses kepada semua server serta sumber-sumber ICT lain; dan

ii. Mewujudkan mekanisma kawalan capaian fizikal untuk staf/individu mencapai server-server yang berkenaan.

14.3.2 Kawalan Capaian Logikal

Kawalan dibuat semasa instalasi agar hanya mereka yang dibenarkan sahaja berupaya mencapai sistem. Di antara mekanisma kawalan capaian adalah seperti berikut:

i. Identifikasi Pengguna

Pengguna sistem boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama. Dalam kedua-dua keadaan, pengguna perlu bertanggungjawab ke atas keselamatan sistem yang digunakan. Di antara langkah-langkah yang diambil untuk mengenalpasti pengguna yang sah ialah:

a. Memberi satu ID yang unik kepada setiap pengguna individu;

b. Menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti;

c. Memastikan adanya kemudahan ‘auditing’ untuk menyemak semua aktiviti pengguna;

d. Memastikan semua ID pengguna yang diwujudkan adalah berpolisikan permohonan dan tiada ID pengguna yang tidak diperlukan; dan

e. Perubahan ID pengguna untuk sistem aplikasi perlu mendapat kebenaran daripada pemilik ('owner') sistem tersebut.

Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan :

a. Menggantung semua kemudahan ('privilege') ID yang tidak digunakan selama 30 hari dan menghapus ID berkenaan selepas dari tempoh 30 hari tersebut; dan

b. Menghapuskan semua kemudahan untuk pengguna yang berpindah atau tamatkan perkhidmatan.

'Audit trail' untuk setiap aktiviti pengguna hendaklah disimpan dan diarkibkan sekiranya keperluan storan adalah mencukupi terutamanya untuk pengguna yang boleh mencapai maklumat sulit agar dapat dikenalpasti sekiranya berlakunya pencerobohan maklumat.

ii. Autentikasi Pengguna

Proses ini adalah untuk mengenalpasti sama ada pengguna tersebut adalah pengguna yang sah melalui penggunaan kata laluan. Panduan pemilihan dan penggunaan kata laluan adalah seperti berikut:

a. Kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat;
b. Panjang kata laluan sekurang-kurangnya 8 aksara;
c. Merupakan kombinasi daripada aksara, angka dan simbol-simbol lain;
d. Dicadang ditukar sekurang-kurangnya tiga (3) bulan sekali;
e. Tidak dikongsi oleh pengguna yang berlainan;
f. Tidak menggunakan kata laluan yang mudah diteka seperti nombor staf, nama pasangan atau anak, nombor plet kereta, dsbnya;
g. Kata laluan dienkrip semasa penghantaran, di mana yang boleh;
h. Fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan
i. Elakkan dari menggunakan semula dua (2) kata laluan terakhir.

iii. Had Cubaan Capaian

Cubaan capaian dihadkan kepada tiga (3) kali sahaja. ID pengguna berkenaan perlu digantung selepas tiga (3) kali cubaan gagal yang berturut.

14.3.3 Audit 'Trail'

'Audit trail' adalah rekod aktiviti yang digunakan untuk mengenalpasti akauntabiliti pengguna sekiranya berlaku sebarang masalah. Penggunaan 'audit trail' untuk sistem komputer dan manual operasi perlu diwujudkan untuk:

i. Capaian kepada maklumat yang kritikal;

ii. Capaian kepada perkhidmatan rangkaian; dan

iii. Keistimewaan atau kebenaran tertentu yang melebihi kebenaran sebagai pengguna biasa digunakan seperti arahan-arahan keselamatan dan fungsi-fungsi 'superuser.'

Maklumat 'audit trail' merangkumi:

i. Identifikasi pengguna;
ii. Fungsi, sumber dan maklumat yang digunakan atau dikemaskini;
iii. Tarikh dan masa;
iv. Alamat IP 'client' atau 'workstation'; dan
v. Transaksi dan program yang dijalankan secara spesifik.

Langkah-langkah keselamatan yang dilakukan dalam menyediakan audit 'trail:

i. Meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera;

ii. Meneliti 'audit trail' secara berjadual;

iii. Meneliti dan melaporkan sebarang masalah berkaitan keselamatan dan sesuatu kejadian yang di luar kebiasaan;

iv. Menyimpan maklumat 'audit trail' untuk jangka masa tertentu untuk keperluan operasi; dan

v. Mengawal maklumat 'audit trail' daripada dihapus, diubahsuai, penipuan atau 're-sequencing'.

14.3.4 'Backup'

Bagi memastikan sistem dapat dipulihkan sepenuhnya jika berlaku sebarang masalah atau kerosakan, proses 'backup' secara berjadual perlu dilakukan termasuk apabila berlakunya perubahan konfigurasi pada sistem pengoperasian. 'Backup' perlu disimpan di dalam bilik yang selamat.

Langkah-langkah bagi penyediaan 'backup' ialah:

i. Prosedur 'backup'/'restore' didokumenkan;

ii. Menyimpan tiga (3) generasi backup';

iii. Menyimpan salinan 'backup' di tempat lain yang selamat; dan

iv. Media 'backup' dan prosedur 'restore' diuji dua (2) kali setahun.

14.3.5 Penyelenggaraan

Bagi memastikan integriti sistem pengoperasian daripada terdedah kepada sebarang pencerobohan keselamatan, laksanakan kawalan-kawalan berikut:

i. 'Patches' dan Kelemahan Sistem ('Vulnerabilities')

'Patches' dan kelemahan sistem sentiasa dijumpai dan bagi mengatasinya, sentiasa dapatkan patches yang terkini daripada agensi keselamatan berdaftar seperti MyCERT (Malaysian Computer Emergency Response Team) di alamat web

http://www.mycert.org.my/.

ii. Peningkatan ('upgrades')

Satu prosedur pengemaskinian sistem pengoperasian daripada serangan dan ancaman diwujudkan.

14.4 Keselamatan Sistem Aplikasi

Semua capaian ke sistem aplikasi mestilah oleh pengguna yang berdaftar. Langkah-langkah pengawalan perlu dilaksanakan bagi menjamin keselamatan sistem.

14.4.1 Perisian Aplikasi

Di dalam perisian aplikasi, kawalan keselamatan perlu dilaksanakan untuk mengelakkan berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. Kawalan tersebut merangkumi:

i. Sistem keselamatan bersepadu dengan kemudahan kawalan capaian di dalam sistem pengoperasian yang membenarkan pengurusan ID pengguna dan kata laluan secara berpusat;

ii. Struktur profil capaian yang mengawal capaian maklumat dan fungsi-fungsi berpolisikan peranan dan keperluan capaian;

iii. Kawalan capaian secara konsisten terhadap maklumat yang di'replicate' kepada pelbagai platform;

iv. Kawalan aplikasi yang menentukan akauntabiliti tertentu kepada setiap pengguna untuk setiap transaksi; dan

v. Polisi kepunyaan ('ownership') kepada maklumat.

14.4.2 Pangkalan Data

Kawalan perlu dilaksanakan untuk menghalang capaian kepada pangkalan data dari sebarang pengubahsuaian atau pemusnahan data secara tidak sah. Integriti maklumat yang disimpan di dalam pangkalan data boleh dikekalkan melalui:

i. Sistem pengurusan pangkalan data yang memastikan integriti dalam pengemaskinian dan capaian maklumat. Kawalan secara serentak perlu untuk pangkalan data yang dikongsi bersama;

ii. Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Sistem;

iii. Mekanisma kawalan capaian kepada sumber maklumat fizikal bagi mengawal capaian kepada sistem pengurusan maklumat, aplikasi dan pengguna; dan

iv. Melaksanakan tugas-tugas rutin pangkalan data seperti:

a. Semakan 'database consistency';
b. Semakan penggunaan ruang storan;
c. Pemantauan aktiviti pangkalan data;
d. Pemantauan aktiviti server dan pengguna ('auditing');

e. Melaksanakan ‘backup/restore’; dan
f. ‘Performance tuning’.

14.4.3 Pengujian Aplikasi

Salah satu aspek pembangunan sistem aplikasi ialah pengujian yang dilaksanakan pada beberapa peringkat iaitu koding aturcara, modul, sistem aplikasi, integrasi sistem aplikasi dan pengujian pengguna. Ia melibatkan pengujian aplikasi baru, penambahbaikan kepada aplikasi semasa atau pemindahan daripada perkakasan lama kepada baru. Pengujian perlu bagi memastikan sistem berfungsi berpolisikan kepada spesifikasi yang ditetapkan.

Bagi menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya semasa pengujian:

i. Gunakan data ‘dummy’ atau ‘historical’ untuk tujuan pengujian;

ii. Mengawal penggunaan data terpilih (‘classified’) semasa pengujian aplikasi;

iii. Kawalan capaian untuk menghadkan capaian kepada kakitangan yang sepatutnya;

iv. Hapuskan maklumat yang digunakan semasa pengujian sistem (terutamanya apabila menggunakan data ‘historical’); dan

v. Menggunakan persekitaran yang berbeza untuk pembangunan sistem dan pengoperasian sistem. Wujudkan persekitaran berasingan untuk pembangunan sistem seperti merekabentuk, membangun, menguji dan mengintegrasi sistem aplikasi.

14.4.4 Perisian yang ‘Malicious’ dan Rosak (‘Defective’)

Pembangunan perisian boleh dikategorikan kepada dua iaitu pembangunan secara dalaman (‘in-house’) atau ‘outsourcing’. Kedua-dua keadaan boleh terdedah kepada perisian yang tidak berfungsi sebagai mana ditetapkan. Kerosakan ini boleh dikesan semasa proses pengujian.

Untuk mengurangkan kemungkinan perisian yang rosak, kawalan berikut perlu dilaksanakan:

i. Sekiranya ‘outsourcing’, dapatkan perisian daripada pembekal yang mempunyai reputasi yang baik, rekod prestasi perkhidmatan yang baik dan mempunyai kepakaran teknikal yang tinggi;

ii. Wujudkan program jaminan kualiti dan prosedur untuk semua perisian yang dibangunkan secara dalaman atau ‘outsourcing’ dari luar; dan

iii. Pastikan semua perisian didokumenkan, diuji, disahkan fungsinya, tahan lasak (‘robustness’) dan menepati spesifikasi.

14.4.5 Perubahan Versi (‘version’)

Versi baru perisian bagi aplikasi, sistem pengoperasian sentiasa dikeluarkan secara berkala bagi mengatasi masalah pepijat dan ancaman serta meningkatkan fungsinya. Perubahan versi perisian perlu dikawal bagi

memastikan integriti perisian apabila perubahan dibuat dan ini memerlukan pematuhan kepada prosedur kawalan perubahan.

14.4.6 Penyimpanan Kod Sumber ('Source Code')

Bagi sistem yang diperolehi dari pembekal luar, kod sumber diperlukan untuk tujuan 'debugging' dan peningkatan sistem. Kawalan penyimpanan merangkumi:

i. Mewujudkan prosedur untuk menyelenggara versi terkini program; dan

ii. Mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada.

14.4.7 Perisian Tidak Berlesen

Perisian tidak berlesan adalah tidak sah. Pastikan penggunaan perisian berlesen dan kawalan inventori seperti menyimpan lesen dengan selamat serta kawalan fizikal ke atas lokasi perisian berlesen dan salinan lesen yang dikeluarkan.

14.4.8 Kod Jahat ('Malicious Code')

Bagi memastikan integriti maklumat daripada pendedahan atau kemusnahan daripada 'malicious code' seperti virus, kawalan berikut perlu digunakan:

i. Melaksanakan prosedur untuk menguruskan 'malicious code';

ii. Mewujudkan polisi berkaitan memuat turun, penerimaan dan penggunaan perisian percuma ('freeware' dan 'shareware');

iii. Menyebarkan arahan dan maklumat untuk mengesan 'malicious code' kepada semua pengguna; dan

iv. Mendapatkan bantuan sekiranya disyaki dijangkiti virus dan lain-lain.

Bagi memastikan keupayaan pemprosesan dapat dipulihkan akibat serangan 'malicious code', beberapa langkah perlu dilaksanakan termasuk:

i. Menyimpan semua salinan utama untuk semua perisian, data dan maklumat untuk tujuan 'restore'; dan

ii. Memastikan semua data di'backup' secara berkala.

Bagi masalah serangan virus, ikuti langkah-langkah berikut:

i. Gunakan perisian anti virus yang telah diluluskan;

ii. Scan virus menggunakan kemudahan yang disediakan oleh perisian anti-virus;

iii. Hapus dan buang virus berkenaan dengan segera;

iv. Menyemak status 'scanning' di dalam laporan log; dan

v. Tidak melaksana (‘run’) atau membuka fail kepilan (‘attachment’) daripada email yang meragukan.

14.5 Keselamatan Penggunaan Email

14.5.1 Akaun Email

i. Akaun email bukan hak mutlak seseorang. Ia adalah kemudahan yang disediakan tertakluk kepada peraturan Universiti dan boleh ditarik balik jika penggunaannya melanggar peraturan;

ii. Gunakan akaun email milik pengguna. Pengguna tidak dibenarkan menggunakan akaun email milik orang lain atau akaun yang dikongsi bersama untuk mengemukakan pendapat persendirian. Pengguna juga tidak digalakkan menggunakan akaun yang didaftarkan secara percuma untuk penghantaran email rasmi; dan

iii. Kata laluan tidak boleh didedahkan kepada pengguna lain. Pendedahan akan membolehkan pengguna lain menyalahgunakan kemudahan tanpa pengetahuan pemilik akaun.

14.5.2 Menyenggara Kotak Mel (‘Mail Box’)

i. Kandungan dan penyelenggaraan kotak mel pada komputer peribadi adalah menjadi tanggungjawab pengguna;

ii. Pengguna harus menghadkan jumlah email yang disimpan di dalam kotak mel. Hapuskan email yang difikirkan tidak perlu disimpan;

iii. Pengguna hendaklah sentiasa mengimbas fail dalam kotak mel dengan perisian anti-virus. Pengguna perlu berhati-hati kerana email adalah cara paling mudah untuk penghantaran virus daripada sebuah komputer ke komputer yang lain. Pengguna juga hendaklah memastikan fail yang akan dihantar melalui lampiran (‘attachment’) bebas daripada virus. Jika tidak, virus boleh merebak dengan cara tidak sengaja dengan meluas; dan

iv. Email juga mungkin terdedah kepada pencerobohan atau dicapai oleh penceroboh (‘hackers’). Email seboleh-bolehnya tidak mengandungi maklumat rahsia yang boleh disalah guna untuk merosakkan akaun, stesyen kerja, komputer server dan rangkaian UNISELNet.

14.5.3 Penggunaan Perisian Mail

i. Pengguna digalakkan mengguna perisian mail rasmi UNISEL yang lebih selamat daripada ancaman dan penyebaran virus berbanding perisian lain seperti Microsoft Outlook, Eudora dan lain-lain; dan

ii. Pengguna yang tidak menggunakan perisian mel rasmi UNISEL dinasihatkan sentiasa membuat ‘backup’ terhadap data-data email.