GARIS PANDUAN KESELAMATAN OPERASI IT DI UNIVERSITI TEKNIKAL MALAYSIA MELAKA

SUSUNAN
GARIS PANDUAN

Perenggan

GARIS PANDUAN KESELAMATAN OPERASI IT DI UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.0 TUJUAN

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

2.0 TAFSIRAN DAN INTERPRETASI

2.1 Dalam Garis Panduan ini, melainkan jika konteksnya menghendaki makna yang lain—

”Garis Panduan” ertinya Garis Panduan Keselamatan Operasi IT di Universiti Teknikal Malaysia Melaka;

”ICT” ertinya *information and communications technology*;

”pengguna” ertinya:-

a) staf - mana-mana orang yang diambil kerja oleh Universiti sama ada secara tetap, kontrak, sementara, sambilan, dan termasuk seseorang yang berkhidmat di Universiti secara pinjaman; dan

b) pelajar - seseorang yang mendaftar sesuatu program akademik (sama ada penuh atau separuh masa atau siswazah) di UTeM dan statusnya masih aktif.

”Pusat Data” ertinya kemudahan yang memusatkan operasi dan peralatan teknologi maklumat organisasi, pusat pengawalan keselamatan data serta tempat menyimpan dan mengurus penyebaran data;

”PPPK” ertinya Pusat perkhidmatan Pengetahuan dan Komunikasi UTeM;

”PTj” ertinya Pusat Tanggungjawab yang terdiri daripada Pejabat/Fakulti/Institut/Pusat atau apa-apa jua nama ia disebut; dan

“UTeM” bermaksud Universiti Teknikal Malaysia Melaka.

2.2 Interpretasi

(a) Mana-mana perkataan dalam bentuk tunggal adalah termasuk juga yang majmuk dan sebaliknya.

(b) Pada bila-bila masa Garis Panduan ini merujuk setiap hari dalam kalendar, apa-apa angka atau nombor tersebut hendaklah dirujuk kepada hari-hari dalam kalendar Gregorian.

(c) Tajuk-tajuk dan tajuk-tajuk kecil dalam Garis Panduan ini dimasukkan bertujuan untuk memudahkan rujukan sahaja dan tidak boleh dibuat pertimbangan dalam mentafsirkan Garis Panduan ini.

(d) Lampiran-lampiran yang dirujuk di dalam Garis Panduan ini (jika ada) hendaklah diambil, dianggap, dibaca dan ditafsirkan sebagai bahagian yang penting kepada Garis Panduan ini.

3.0 SKOP

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

4.0 KESELAMATAN SISTEM KOMPUTER/*SERVER*

4.1 Kawalan Capaian Fizikal

4.1.1 Kawalan terhadap pengguna yang masuk ke Pusat Data dan juga kawalan akses perkakasan dan perisian dalam Pusat Data.

4.1.2 Mewujudkan mekanisma kawalan capaian fizikal untuk pengguna mencapai maklumat yang dihasilkan di Pusat Data.

4.2 Kawalan Capaian Logikal

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

4.2.1 Identifikasi Pengguna

Pengguna sistem hendaklah bertanggungjawab atas keselamatan sistem yang digunakan. Antara langkah-langkah yang diambil untuk mengenalpasti pengguna yang sah adalah seperti berikut:-

4.2.1.1 Memberi satu ID yang unik kepada pengguna individu;

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

4.2.1.3 Memastikan adanya kemudahan *auditing* untuk menyemak semua aktiviti pengguna;

4.2.1.4 Memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan dan tiada ID pengguna yang tidak diperlukan; dan

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

Bagi pengguna yang tidak aktif (bersara atau berhenti) PPPK akan menghapuskan semua kemudahan bagi tujuan keselamatan.

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

4.2.2 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:-

4.2.2.1 Kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat;
4.2.2.2 Panjang kata laluan sekurang-kurangnya 8 aksara;
4.2.2.3 Kata laluan adalah Kombinasi huruf besar, huruf kecil, simbol dan nombor,
4.2.2.4 Kata laluan hendaklah ditukar sekurang-kurangnya tiga (3) bulan sekali;
4.2.2.5 Tidak dikongsi oleh pengguna yang lain;
4.2.2.6 Tidak menggunakan kata laluan yang mudah diteka seperti nombor staf, nama pasangan atau anak, nombor plet kereta, dan sebagainya;
4.2.2.7 Kata laluan dienkrip semasa penghantaran;
4.2.2.8 Kuat kuasa pertukaran kata laluan semasa *log in* kali

pertama atau selepas kata laluan diset semula;

4.2.2.9 Fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan

4.2.2.10 Mengelakkan penggunaan semula kata laluan semasa dengan kata laluan yang baharu.

4.2.3 Had Cubaan Capaian

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

4.3 *Audit Trail*

4.3.1 *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:-

4.3.3.1 Capaian kepada maklumat yang kritikal;

4.3.3.2 Capaian kepada perkhidmatan rangkaian; dan

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

4.3.2 Maklumat *audit trail* merangkumi:-

4.3.2.1 Identifikasi pengguna;

4.3.2.2 Fungsi, sumber dan maklumat yang digunakan atau dikemaskini;

4.3.2.3 Tarikh dan masa;

4.3.2.4 Alamat IP *client* atau *workstation*; dan

4.3.2.5 Transaksi dan program yang dijalankan secara spesifik.

4.3.3 Langkah-langkah keselamatan yang dilakukan dalam menyediakan *audit trail*:-

4.3.3.1 Meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera;

4.3.3.2 Meneliti *audit trail* secara berjadual;

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

4.3.3.4 Menyimpan maklumat *audit trail* untuk jangka masa tertentu untuk keperluan operasi; dan

4.3.3.5 Mengawal maklumat *audit trail* daripada dihapus, diubahsuai, penipuan atau *re-sequencing*.

4.4 *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:-

4.4.1 Prosedur *backup/restore* didokumenkan;

4.4.2 Menyimpan salinan *backup* di tempat lain yang selamat; dan

4.4.3 Media *backup* dan prosedur *restore* diuji dua (2) kali setahun.

4.5 Penyelenggaraan

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

4.5.1 *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).

4.5.2 Peningkatan *(upgrades)*

Satu prosedur pengemaskinian sistem pengoperasian daripada serangan dan ancaman diwujudkan.

5.0 KESELAMATAN SISTEM APLIKASI

Hanya pengguna sahaja yang dibenarkan untuk mencapai sistem aplikasi UTeM bagi menjamin keselamatan sistem. Di antara langkah-langkah pengawalan yang perlu dilaksanakan bagi menjamin keselamatan sistem adalah seperti berikut:-

5.1 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:-

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

5.1.2 Struktur profil capaian yang mengawal capaian maklumat dan fungsi-fungsi berdasarkan peranan dan keperluan capaian;

5.1.3 Kawalan capaian secara konsisten terhadap maklumat yang di *replicate* kepada pelbagai platform;

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

5.1.5 Dasar kepunyaan *(ownership)* kepada maklumat.

5.2 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:-

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

5.2.2 Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Sistem;

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

5.2.4 Melaksanakan tugas-tugas rutin pangkalan data seperti:-

5.2.4.1 Semakan *database consistency*;

5.2.4.2 Semakan penggunaan ruang storan;

5.2.4.3 Pemantauan aktiviti pangkalan data;

5.2.4.4 Pemantauan aktiviti server dan pengguna *(auditing)*;

5.2.4.5 Melaksanakan *backup/restore*; dan

5.2.4.6 *Performance tuning.*

5.3 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 berdasarkan kepada spesifikasi yang ditetapkan. Berikut adalah langkah-langkah untuk menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya semasa pengujian:-

5.3.1 Menggunakan data *dummy* atau *historical* untuk tujuan pengujian;

5.3.2 Mengawal penggunaan data terpilih *(classified)* semasa pengujian aplikasi;

5.3.3 Kawalan capaian untuk menghadkan capaian kepada kakitangan yang sepatutnya;

5.3.4 Hapuskan maklumat yang digunakan semasa pengujian sistem (terutamanya apabila menggunakan data *historica*l); dan

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

5.4 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:-

5.4.1 Sekiranya *outsourcing*, dapatkan perisian daripada pembekal yang mempunyai reputasi yang baik, rekod prestasi perkhidmatan yang baik dan mempunyai kepakaran teknikal yang tinggi;

5.4.2 Mewujudkan program jaminan kualiti dan prosedur untuk semua perisian yang dibangunkan secara dalaman atau *outsourcing* dari luar; dan

5.4.3 Memastikan semua perisian didokumenkan, diuji, disahkan fungsinya, tahan lasak *(robustness)* dan menepati spesifikasi.

5.5 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.

5.6 Penyimpanan Kod Sumber *(Source Code)*

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

5.6.1 Mewujudkan prosedur untuk menyelenggara versi terkini program; dan

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

5.7 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.

5.8 Kod Jahat *(Malicious Code)*

5.8.1 Bagi memastikan integriti maklumat daripada pendedahan atau kemusnahan daripada *malicious code* seperti virus, kawalan berikut perlu dilaksanakan:-

5.8.1.1 Melaksanakan prosedur untuk menguruskan *malicious code;*

5.8.1.2 Mewujudkan polisi berkaitan memuat turun, penerimaan dan penggunaan perisian percuma *(freeware dan shareware)*;

5.8.1.3 Menyebarkan arahan dan maklumat untuk mengesan *malicious code* kepada semua pengguna; dan

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

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

5.8.2.1 Menyimpan semua salinan utama untuk semua perisian, data dan maklumat untuk tujuan *restore;* dan

5.8.2.2 Memastikan semua data di *backup* secara berkala.

5.8.3 Bagi masalah serangan virus, langkah-langkah berikut hendaklah dipatuhi:-

5.8.3.1 Menggunakan perisian anti virus yang telah diluluskan;

5.8.3.2 *Scan* virus menggunakan kemudahan yang disediakan oleh perisian anti-virus;

5.8.3.3 Hapus dan buang virus berkenaan dengan segera;

5.8.3.4 Menyemak status *scanning* di dalam laporan log; dan

5.8.3.5 Tidak melaksana *(run)* atau membuka fail kepilan *(attachment)* daripada mel elektronik yang meragukan.

6.0 LAIN-LAIN

6.1 Garis Panduan ini adalah tertakluk kepada dasar, pekeliling, surat pekeliling, kaedah, peraturan, dan undang-undang lain yang berkaitan yang berkuat kuasa.

6.2 Garis Panduan ini adalah tertakluk kepada pindaan oleh pihak UTeM dari semasa ke semasa.