GARIS PANDUAN KESELAMATAN VIRUS DI UNIVERSITI TEKNIKAL MALAYSIA MELAKA

SUSUNAN
GARIS PANDUAN

Perenggan

1. Tujuan

2. Tafsiran dan Interpretasi

3. Skop

4. Keselamatan Virus

5. Lain-Lain

GARIS PANDUAN KESELAMATAN VIRUS DI UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.0 TUJUAN

Tujuan Garis Panduan ini adalah untuk memastikan pengawalan dan pengurusan keselamatan dari serangan virus di UTeM.

2.0 TAFSIRAN DAN INTERPRETASI

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

”Garis Panduan” ertinya Garis Panduan Keselamatan Virus Di Universiti Teknikal Malaysia Melaka;

”pengguna” ertinya:-

a) staf - mana-mana orang yang diambil kerja oleh UTeM sama ada secara tetap, kontrak, sementara, sambilan, dan termasuk seseorang yang berkhidmat di UTeM dan luar UTeM 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.

”pengguna luar” ertinya selain pengguna;

”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

Garis Panduan ini merangkumi rangkaian dan perisian seperti sistem komputer, sistem pengoperasian, pangkalan data dan sistem aplikasi.

4.0 KESELAMATAN VIRUS

4.1 Rangkaian

4.1.1 Semua peralatan rangkaian yang akan ke rangkaian luar dan *server farm* perlu melalui sistem keselamatan di PPPK. Sistem ini akan membuat pengauditan melalui *firewall*, *IDS* dan *antivirus gateway* di PPPK.

4.1.2 Setiap *service* dan *port* yang akan ke rangkaian luar dan *server farm* perlu mendapat kelulusan daripada Pengarah PPPK.

4.1.3 Apabila berlaku serangan virus di rangkaian UTeM, PPPK berhak menutup rangkaian kawasan setempat (LAN) yang terlibat.

4.2 Sistem Operasi

Setiap sistem pengoperasian di UTeM perlu di *update (patches)* jika pihak *vendor* seperti *Microsoft* dan *RedHat* mengeluarkan *patches* terkini terhadap *bug* yang ada dalam sistem pengoperasian mereka.

a) Setiap pemilik komputer/*server* bertanggungjawab untuk membuat proses *windows update*.

b) PTj yang mempunyai makmal bertanggungjawab ke atas komputer/*server* makmal untuk membuat proses *windows update*.

c) Pengguna tidak dibenarkan membuka *service* yang tidak berkaitan dalam sistem pengoperasian mereka.

d) Pengguna hendaklah memastikan sistem operasi sentiasa berada pada keadaan terkini dengan melakukan *windows update* dan *software*

update.

e) Pemberitahuan mengenai *patches* yang terkini akan dihebahkan oleh PPPK kepada pengguna sekiranya terdapat situasi yang memerlukan *patches/hotfix* perlu dikemaskini oleh pengguna.

4.3 Antivirus

Setiap sistem pengoperasian di UTeM perlu di *install* dengan perisian antivirus yang disediakan oleh PPPK.

a) Setiap pengguna komputer/server bertanggungjawab memastikan komputer/server mereka telah di *install* dengan perisian antivirus (*pattern* dan *scan engine* terkini) yang disediakan oleh PPPK.

b) Jabatan dan fakulti yang mempunyai makmal bertanggungjawab memastikan komputer/server telah di *install* dengan perisian antivirus (*pattern* dan *scan engine* terkini).

c) PPPK berhak mengambil komputer pengguna jika mendapati komputer/server itu menyebarkan virus.

d) PPPK tidak bertanggungjawab ke atas data jika komputer/server tersebut diserang virus akibat sistem pengoperasian yang tidak mempunyai perisian antivirus.

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 tersebut boleh terdedah kepada perisian yang tidak berfungsi sebagaimana ditetapkan. Pengguna perlu menguji perisian tersebut untuk mengelakkan

perisian itu boleh mengganggu rangkaian dan sistem operasi komputer. PPPK tidak bertanggungjawab jika perisian ini akan menyebabkan kerosakkan sistem operasi komputer tersebut.

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.

4.6 Perisian Tidak Berlesen

Pengurusan perisian tidak berlesen 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.

4.7 Kod Jahat *(Malicious Code)*

4.7.1 Bagi memastikan integriti maklumat daripada pendedahan atau kemusnahan daripada *malicious code* seperti virus maka kawalan berikut perlu digunakan:-

a) Melaksanakan prosedur untuk menguruskan *malicious code*;

b) Menyebarkan arahan, kempen kesedaran dan maklumat untuk mengesan *malicious code* kepada semua pengguna; dan

c) Mendapatkan bantuan sekiranya disyaki dijangkiti virus.

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

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

b) Memastikan semua data mempunyai *backup* secara berkala.

4.7.3 Bagi masalah serangan virus, ikuti langkah-langkah berikut:

a) Gunakan perisian antivirus yang telah diluluskan;

b) *Scan* virus menggunakan kemudahan yang disediakan oleh perisian antivirus;

c) Hapus dan buang virus berkenaan dengan segera;

d) Menyemak status *scanning* di dalam laporan *log*; dan

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

5.0 LAIN-LAIN

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

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