GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (TMK) Universiti Sains Malaysia

KANDUNGAN

1 Pendahuluan

1.1 Pengenalan

Pada masa kini institusi semakin bergantung kepada penggunaan sistem automasi Teknologi Maklumat dan Komunikasi (TMK) bagi memproses maklumat untuk menyokong operasi harian dengan lebih baik. Program keselamatan TMK yang berkesan adalah penting untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat. Memandangkan ancaman keselamatan yang semakin meningkat dan kerumitan dalam sistem TMK yang digunakan, maka Pentadbir TMK mestilah sentiasa memastikan bahawa risiko keselamatan TMK diurus dengan sewajarnya. Selain melaksana kawalan teknikal, amalan operasi dan pentadbiran yang mantap amat penting bagi memastikan pelaksanaan program keselamatan TMK berkesan.

Garis Panduan ini mendefinisikan keperluan mengekalkan tahap keselamatan minimum bagi sistem TMK yang digunakan dalam menyokong operasi di universiti, dan tertakluk kepada semakan berkala. Universiti Sains Malaysia (USM) mempunyai hak untuk mengemas kini dokumen ini apabila perlu.

1.2 Tujuan

Tujuan utama buku panduan ini adalah:

a) menggariskan tanggungjawab Pentadbir TMK terhadap keselamatan TMK; dan
b) memberikan garis panduan dan prosedur kepada Pentadbir TMK untuk mengurus, melaksana dan mengekal keselamatan maklumat di USM berdasarkan Dasar Teknologi Maklumat & Komunikasi (DTMK) dan Perintah Am Kerajaan Malaysia.

1.3 Tanggungjawab

Pentadbir TMK dikehendaki:

a) bertindak selaku pegawai perhubungan bagi semua perkara berkaitan dengan keselamatan TMK;

b) menerangkan keperluan keselamatan dan melaksanakan kawalan menurut dasar dan garis panduan yang disediakan oleh Universiti Sains Malaysia atau Kerajaan Malaysia dari semasa ke semasa;
c) melaporkan kepada PPKT tentang insiden keselamatan, kelemahan keselamatan dan kerosakan sistem TMK supaya tindakan baik pulih dapat dijalankan dengan segera;
d) memasang, mengkonfigurasi dan mentadbir semua sistem TMK yang terdapat di universiti;
e) menganjur program kesedaran keselamatan TMK bagi warga kampus;
f) mengurus dan mengkaji semula hak capaian pengguna;
g) menjalankan semakan pematuhan atau penilaian kendiri;
h) memantau penggunaan sistem dan mengkaji log peristiwa *(event log)* dan jejak audit *(audit trail)* untuk mengesan penyalahgunaan atau insiden keselamatan TMK yang mungkin berlaku; dan
i) menyelenggara semua perisian dan perkakasan yang digunakan, dan memastikan fail tampalan *(patches)* adalah versi terkini serta berfungsi dengan baik.

1.4 Struktur Buku Panduan

Struktur buku panduan ini seperti berikut:

a) Pengurusan Capaian Pengguna menetapkan garis panduan dan prosedur untuk mengurus akaun pengguna. Topik ini menerangkan secara terperinci tentang proses pendaftaran, pembatalan pendaftaran, penyelenggaraan akaun, menyemak semula hak capaian pengguna dan melaksanakan mekanisme kawalan capaian yang lain.
b) ***Backup*** menetapkan keperluan dan proses *penyalinan* yang perlu dilaksanakan serta dipatuhi oleh Pentadbir TMK.
c) **Semakan Semula Pematuhan** menetapkan senarai semak penilaian kendiri yang perlu dilaksanakan oleh Pentadbir TMK.
d) **Pemantauan Keselamatan** menetapkan proses penggunaan sistem pemantauan dan tindakan yang mungkin diambil apabila berlaku pelanggaran keselamatan TMK.

e) **Kesedaran Keselamatan** memberikan garis panduan untuk merangka program kesedaran keselamatan TMK.

f) **Pengendalian Insiden Keselamatan** menetapkan garis panduan dan prosedur untuk bertindak balas terhadap insiden keselamatan TMK, dan keperluan pelaporan berdasarkan DTMK USM.

g) **Kawalan Perubahan *(change control)*** menetapkan garis panduan dan prosedur bagi mengurus perubahan dalam perisian, perkakasan, sistem telekomunikasi dan dokumentasi.

h) **Pelaksanaan *Anti-malicious Code*** menentukan matlamat dan strategi pelaksanaan *anti-malicious code*.

i) **Keselamatan Fizikal Infrastruktur TMK** menetapkan garis panduan kepada Pentadbir TMK dalam penyediaan bilik server.

2 Pengurusan Capaian Pengguna

2.1 Pengenalan

Proses pengurusan capaian pengguna yang berkesan amat penting untuk mengelakkan capaian tanpa kebenaran terhadap maklumat dan sistem TMK. Garis panduan pengurusan capaian pengguna ini mencakupi semua peringkat dalam kitar hayat capaian pengguna, bermula dari peringkat pendaftaran pengguna baru hinggalah pembatalan akaun pengguna yang tidak lagi perlu mengakses sistem dan perkhidmatan dan sistem maklumat.

2.2 Tujuan

Topik ini bertujuan menguruskan pengguna, mengawal capaian maklumat dan sistem TMK. Pengurusan ini termasuk kawalan dan pencegahan capaian tanpa kebenaran. Selain itu, topik ini juga memberi garis panduan kepada Pentadbir TMK untuk mengurus kitar hayat capaian pengguna.

2.3 Garis Panduan

2.3.1 Pendaftaran/Pembatalan Akaun Pengguna

a) Setiap pengguna seharusnya diberi satu akaun pengguna dengan identiti (ID) yang unik dan kata laluan permulaan. Hal ini untuk memastikan pengguna sendiri bertanggungjawab bagi sebarang aktiviti yang melibatkan penggunaan ID mereka.

b) Satu proses pendaftaran pengguna untuk mengakses sistem TMK mestilah ditentukan oleh Pentadbir TMK. Pentadbir TMK boleh menimbang untuk menggunakan borang permohonan, atau mekanisma lain yang dianggap sesuai.

c) Kumpulan dan peranan pengguna mestilah ditentukan dan disahkan terlebih dahulu.

d) Perolehan capaian mestilah difailkan atau direkodkan. Rekod ini akan menjadi jejak audit untuk rujukan pada masa depan.

e) Pentadbir TMK hendaklah dengan segera menyelaraskan akaun pengguna yang berpindah atau berhenti dari menjadi warga USM. Pembatalan akaun pengguna mestilah disahkan dan dilaksanakan atas sebab-sebab yang dinyatakan. Dicadangkan supaya akaun pengguna digantung selama enam (6) bulan sebelum dihapuskan.

2.3.2 Pengurusan Peranan dan Hak Capaian *(Privilege Management)*

a) Kawalan capaian adalah berasaskan peranan samada pelajar, pensyarah, penyelidik, pengurusan dan pentadbir sistem. Mekanisme ini melibatkan kumpulan pengguna dan hak capaian yang telah ditentukan terlebih dahulu oleh sistem.

b) Pentadbir TMK dicadangkan meminimumkan perubahan peranan dan hak capaian bagi setiap kumpulan kecuali diwajarkan mengikut keperluan urusan dan dibenarkan oleh CIO atau universiti.

c) Capaian kepada sistem atau maklumat hendaklah dibenarkan hanya pada tahap yang diperlukan oleh fungsi kerja atau peranan pengguna untuk menyelesaikan fungsi kerja tersebut.

d) Dicadangkan akaun lain dengan peranan dan hak pentadbir *(Administrator)* diwujudkan supaya semasa ketiadaan Pentadbir TMK dan pemegang akaun tersebut boleh memainkan peranan sokongan dengan persetujuan CIO.

2.3.3 Penyelenggaraan Akaun Pengguna

a) Sekiranya pengguna terlupa kata laluan, permohonan untuk set semula kata laluan berkenaan hendaklah dihantar kepada CIO. Permintaan tersebut hendaklah direkodkan atau difailkan (jika menggunakan borang). Setiap pengguna baru hendaklah diberi kata laluan permulaan yang mesti ditukar semasa log masuk kali pertama.

b) Sekiranya peranan pengguna bertukar (disebabkan kenaikan pangkat atau apa-apa sebab lain), Pentadbir TMK perlu mengkaji semula peranan dan hak capaian pengguna untuk mengakses sistem. Mana-mana permohonan pertukaran sedemikian hendaklah dibenarkan dan direkodkan atau difailkan (jika menggunakan borang).

2.3.4 Pengurusan Kata Laluan Pengguna

a) Peraturan kata laluan berikut mestilah dikuatkuasakan oleh CIO:

i. kata laluan mestilah mempunyai sekurangkurangnya lapan (8) aksara;

ii. kata laluan mestilah mengandungi sekurang-kurangnya 3 set alphanumerik yang dipilih dari huruf besar, huruf kecil, nombor dan simbol

p@55w07D;

iii. pengguna akan diminta untuk menukar kata laluan mereka semasa log masuk kali pertama;

iv. kata laluan seboleh-bolehnya diperbaharui setiap 180 hari atau lebih kerap; dan

v. kata laluan tidak boleh dikongsi dengan pengguna-pengguna, servis-servis atau laman-laman sesawang yang lain.

b) Setiap ID pengguna mestilah dipautkan kepada kata laluan yang hanya diketahui oleh pengguna tersebut.

2.3.5 Semakan Semula Hak Capaian Pengguna

a) Bagi memastikan kawalan yang berkesan dalam mencapai maklumat dan sistem TMK, Pentadbir TMK perlu:

   i. mengkaji semula hak capaian pengguna sekurang-kurangnya setiap enam (6) bulan; dan
   ii. menyemak hak capaian istimewa (misalnya akaun *root user* atau akaun pentadbir) sekurang-kurangnya setiap tiga (3) bulan.

b) Pentadbir TMK hendaklah membatalkan serta-merta hak capaian mana-mana pengguna, sekiranya berlaku sebarang penyalahgunaan atau capaian tanpa kebenaran.

2.3.6 Pelaksanaan Kawalan Capaian

a) Capaian kepada sistem hendaklah dibuat melalui satu proses yang selamat untuk meminimumkan capaian tanpa kebenaran. Sistem hendaklah dikonfigurasi supaya memaparkan notis amaran am yang menyatakan hanya pengguna yang sah sahaja boleh mengakses komputer.
b) Pengguna akan dilog keluar secara automatik oleh sistem selepas tempoh maksimum yang ditentukan bagi skrin melahu (contohnya 10 minit),
c) Pengguna akan dihalang daripada memasuki sistem sekiranya gagal log masuk tiga (3) kali berturut-turut.

2.3.7 Pelaksanaan Polisi Kumpulan *(Group Policy)*

a) Pentadbir TMK hendaklah menentukan polisi bagi kumpulan, pengguna dan mesin untuk mengawal capaian kepada sumber.
b) Semua stesen kerja dan server hendaklah dikonfigurasikan untuk menerima pelbagai polisi pengguna atau unit organisasi (OU).

3 Backup

3.1 Pengenalan

Backup bertujuan memastikan data dan sistem boleh dipulihkan setelah berlakunya bencana atau kegagalan media.

3.2 Tujuan

Topik ini bertujuan membantu Pentadbir TMK melaksanakan proses *backup*, penstoran semula *(restore)* dan pelan pemulihan bencana *(disaster recovery)* secara berkesan.

3.3 Garis Panduan

3.3.1 Penstoran Media *Backup* di Luar Kawasan *(offsite)*

a) Item berikut hendaklah disimpan di tempat yang berasingan, dan pada jarak yang bersesuaian untuk mengelakkan sebarang kerosakan akibat bencana di tapak utama:

   i. Rekod backup yang tepat dan lengkap.
   ii. Dokumen prosedur penstoran semula (restore).
   iii. Sekurang-kurangnya tiga (3) generasi atau kitar media backup.

b) Media *backup* hendaklah diberikan tahap perlindungan fizikal dan persekitaran yang bersesuaian selaras dengan piawaian yang digunakan di bilik server. Kawalan yang digunakan untuk media di bilik server hendaklah meliputi media storan di luar kawasan.

3.3.2 Pengujian Media *Backup*

Media *backup* hendaklah diuji untuk memastikan kebolehgunaan media itu apabila diperlukan ketika kecemasan.

3.3.3 Penyemakan Prosedur Penstoran Semula *(Restore)*

Prosedur penstoran semula hendaklah sentiasa disemak dan diuji untuk memastikan proses penstoran semula ini berkesan dan boleh disempurnakan mengikut masa yang ditetapkan**.**

3.3.4 Jadual *Backup*

a) *Backup* data hendaklah dilakukan dengan menggunakan skema kitaran *five (5) days differential Grandfather-Father-Son (GFS)*.
b) *Backup* keseluruhan sistem dan disket pemulihan bencana mestilah dilaksanakan setiap enam (6) bulan.
c) Semua *backup* hendaklah dijadualkan pada luar waktu puncak (misalnya pada waktu malam).

3.3.5 Kitaran Media dan Tempoh Penyimpanan

a) Pentadbir TMK hendaklah melaksanakan skema kitaran *five (5) days differential Grandfather-Father-Son (GFS)*.
b) Media yang mengandungi *backup* keseluruhan sistem hendaklah disimpan selama satu (1) tahun.

3.3.6 Pelabelan Media

Setiap media *backup* hendaklah dilabel dengan sempurna selepas Pentadbir TMK selesai membuat *backup* bagi memastikan media yang betul digunakan untuk tujuan yang dimaksudkan. Label itu mestilah mengandungi nama pemilik, tarikh dan identiti server (jika perlu).

4 Semakan Semula Pematuhan *(Compliance Review)*

4.1 Pengenalan

Semakan semula pematuhan secara berkala merupakan mekanisme untuk Pentadbir TMK menentukan status program keselamatan TMK. Jika perlu, kelemahan dikenal pasti

bagi tujuan penambahbaikan. Kajian ini juga menjadi mekanisme bagi USM mengumpul maklum balas tentang keberkesanan program keselamatan sedia ada daripada Pentadbir TMK.

4.2 Tujuan

Topik ini bertujuan memberikan garis panduan berprosedur bagi Pentadbir TMK untuk:

a) melakukan semakan semula pematuhan setiap enam (6) bulan;
b) memantau bidang kawalan dengan lebih cekap; dan
c) mengkaji semula senarai semak pematuhan penilaian kendiri.

4.2.1 Garis Panduan

4.2.2 Semakan Semula Pematuhan Secara Berkala

a) Pentadbir TMK hendaklah melakukan semakan semula pematuhan secara berkala untuk memastikan pelaksanaan kawalan keselamatan TMK mematuhi garis panduan berprosedur yang diberikan oleh CIO dan dokumen ini.
b) Pentadbir TMK hendaklah merekodkan justifikasi bagi setiap penyalahgunaan (atau ketidakpatuhan) yang telah dipertimbangkan.
c) Pentadbir TMK hendaklah sentiasa menambah baik infrastruktur keselamatan berdasarkan syor dan nasihat daripada pihak berkuasa yang berkenaan.

4.2.3 Proses Kajian Semakan Semula

a) Kajian semula pematuhan hendaklah berbentuk soal selidik *(Lihat **Lampiran A - Senarai Semakan Semula Pematuhan**)* yang perlu dilengkapkan oleh Pentadbir TMK.
b) CIO berhak untuk membenar atau tidak membenar pengecualian pematuhan setelah mengambil kira risiko keselamatan.

c) Pentadbir TMK akan dimaklumkan oleh CIO tentang keputusan tersebut secara bertulis bersama-sama syor bagi menepati pematuhan (jika pengecualian tidak dibenarkan).

d) Kajian semula pematuhan mestilah dijalankan setiap enam (6) bulan dan keputusannya hendaklah dimaklumkan kepada CIO/Majlis Teknologi Maklumat

5 Pemantauan Keselamatan *(Security Monitoring)*

5.1 Pengenalan

Pemantauan keselamatan melibatkan semakan berkala terhadap keseluruhan sistem TMK, contohnya aktiviti pengguna. Dapatan pemantauan ini membolehkan Pentadbir TMK mengambil langkah proaktif dan dapat meminimumkan risiko sebelum keadaan menjadi lebih rumit.

5.2 Tujuan

Topik ini bertujuan memberikan garis panduan dan prosedur bagi Pentadbir TMK untuk:

a) memantau penggunaan sistem dan pelanggaran polisi penggunaan yang diterima pakai;

b) mengenal pasti dan menentukan bidang yang akan dipantau serta tindakan yang perlu diambil apabila pelanggaran polisi dikesan.

5.3 Garis Panduan

5.3.1 Bidang Pemantauan Keselamatan

a) Log sistem hendaklah disemak dan dikaji oleh Pentadbir TMK untuk menentukan aktiviti biasa dan luar biasa dalam sistem TMK.

b) Bidang yang patut dipertimbangkan untuk pemantauan termasuklah:

i. Capaian yang dibenarkan, termasuk butiran seperti berikut:

- ID pengguna;
- tarikh dan masa peristiwa penting;

- jenis peristiwa;
- fail yang dicapai; dan
- program/utiliti yang digunakan

ii. Semua operasi khusus, seperti

- penggunaan akaun pentadbir;
- pemula dan penghenti sistem; dan
- memasang/menanggal peranti I/O.

iii. Percubaan capaian tanpa kebenaran, seperti

- percubaan yang gagal;
- pelanggaran polisi capaian; dan
- amaran daripada *firewall* atau system pengesanan pencerobohan (jika ada)

iv. Amaran atau kegagalan sistem, seperti

- amaran atau mesej; dan
- pengecualian log sistem.

v. Log server proksi *(Proxy Server)*

Pentadbir TMK hendaklah melihat dan menyemak log capaian secara berkala. Kekerapan semakan semula hendaklah bergantung pada risiko yang terlibat.

vi. Bagi pemantauan yang berkesan, perisian seperti *spam filtering*, sistem pengesanan pencerobohan dan *firewall* disyorkan untuk menangani serangan baru dan kompleks terhadap sistem TMK.

5.3.2 Respon kepada Salah Guna

Langkah-langkah berikut hendaklah diikuti:

i. Mengesan nama pengguna yang melanggar tata cara penggunaan e-mel atau internet yang diterima pakai.
ii. Merekodkan tarikh dan masa pengesanan itu.
iii. Menyimpan log berkenaan sebagai bukti untuk masa depan.
iv. Menghalang pengguna daripada melaksanakan aktiviti tanpa kebenaran dengan menyekat capaian.

v. Melengkapkan notis pemberitahuan salah guna.

(*Lihat* ***Lampiran B: Contoh Notis Pemberitahuan Bagi Penyalahgunaan Sumber TMK***)

vi. Menghantar notis pemberitahuan salah guna kepada CIO.

vii. Memberikan butiran terperinci tentang penyalahgunaan jika diminta oleh CIO.

viii. Mengambil tindakan terhadap individu yang terlibat setelah berunding dengan CIO, contohnya menggantung akaun pengguna bagi satu tempoh tertentu.

5.3.3 Respon kepada Berpotensi Insiden Keselamatan

a) Pentadbir TMK hendaklah memerhati perlakuan pengguna yang luar biasa dan membuat penyiasatan jika perlu.

b) Kelakuan pengguna yang luar biasa memungkinkan berlakunya pelanggaran atau insiden keselamatan berpotensi. Pentadbir TMK hendaklah mendapatkan lebih banyak bukti sebelum mengambil sebarang tindakan terhadap pengguna tersebut. Pentadbir TMK tidak boleh berbincang kejadian tersebut dengan sesiapa pun kerana ini akan mengakibatkan pengguna yang disyaki mengetahui tentang perkara tersebut.

c) Jika hasil siasatan menunjukkan bahawa kejadian itu hanyalah penyalahgunaan biasa, maka Pentadbir TMK hendaklah merujuk **Perkara 5.3.2** untuk tindakan selanjutnya.

d) Jika kejadian itu merupakan insiden keselamatan berpotensi, maka Pentadbir TMK hendaklah menanganinya mengikut **Perkara 7.4**.

6 Kesedaran Keselamatan *(Security Awareness)*

6.1 Pengenalan

Kesedaran keselamatan dalam kalangan pengguna akan membawa kepada pemahaman yang jelas tentang tanggungjawab mereka untuk mematuhi polisi keselamatan TMK dan menggalakkan amalan keselamatan yang baik.

6.2 Tujuan

Topik ini bertujuan memberi panduan berkaitan pembangunan dan penyebaran program kesedaran keselamatan bagi meningkatkan kesedaran serta memupuk kemahiran dan pengetahuan tentang keselamatan.

6.3 Garis Panduan

6.3.1 Merancang Program Kesedaran Keselamatan

Program kesedaran hendaklah mengambil kira latar belakang pendidikan, bidang kerja dan pelepasan keselamatan *(security clearance)* yang berlainan untuk mendapatkan manfaat maksimum bagi semua kumpulan sasar. Oleh itu, langkah-langkah berikut hendaklah diambil apabila merancang program kesedaran keselamatan:

a) Mengenal pasti kumpulan sasar kepada siapa usaha kesedaran keselamatan ini akan ditujukan.
b) Mengenal pasti tujuan dan objektif mengadakan program kesedaran keselamatan.
c) Mengenal pasti tajuk program kesedaran keselamatan berdasarkan keperluan.
d) Mengenal pasti mekanisme atau kaedah penyampaian yang berlainan sesuai mengikut tujuan kesedaran.
e) Mengukur keberkesanan program kesedaran

(Lihat Lampiran C: Contoh Penilaian Program Kesedaran)

6.3.2 Kekerapan Program Kesedaran Keselamatan

Kesedaran keselamatan merupakan proses berterusan. Oleh yang demikian, sekurang-kurangnya satu (1) program kesedaran mestilah dijalankan dalam setahun.

6.3.3 Komponen Program Kesedaran Keselamatan

Satu program kesedaran yang dirancang dengan baik hendaklah mengandungi semua komponen yang digariskan dalam jadual di bawah:

	Kesedaran	**Latihan & Akultrasi**	**Pendidikan**
Sifat	"Apa"	"Bagaimana"	"Mengapa"
Peringkat	Maklumat	Pengetahuan	Pemerhatian
Objektif	Perakuan	Kemahiran & Pengalaman	Pemahaman
Kaedah Mengajar	Media • Video • Surat Berita • Poster • Ceramah • Seminar	Pengajaran Praktikal • Ceramah • Kajian kes dan bengkel • Amali • Kaunseling	Pengajaran secara teori • Perbincangan • Seminar • Melalui Pembacaan • Kempen
Ukuran Ujian	• Pemahaman • Temubual • Kajian kes • Kaunseling	• Penyelesaian masalah (Aplikasi) Pembelajaran • Pentauliahan	Pertandingan menulis esei
Tempoh Masa	Jangka pendek	Pertengahan	Jangka Panjang

7 Pengendalian Insiden Keselamatan *(Security Incident Handling)*

7.1 Pengenalan

Ancaman keselamatan yang semakin banyak mengganggu sistem TMK menyebabkan proses menangani sesuatu insiden itu menjadi amat penting untuk mengurangkan kehilangan dan kerosakan. Pentadbir TMK mestilah mengambil tindakan baik pulih bagi menyelesaikan masalah. Information Technology Infrastructure Library (ITIL) merupakan piawaian antarabangsa yang terbaik untuk diaplikasikan di Universiti Sains Malaysia .

7.2 Tujuan

Topik ini bertujuan memberi garis panduan dan prosedur bagi pengendalian insiden keselamatan oleh Pentadbir TMK untuk:

a) menangani insiden atau pelanggaran keselamatan; dan
b) meminimumkan kerosakan akibat insiden keselamatan dan kegagalan fungsi *(malfunction)*.

7.3 Garis Panduan

7.3.1 Peraturan Am

a) Tanggungjawab dan prosedur menangani kejadian hendaklah ditentukan untuk memastikan respon segera, berkesan dan teratur terhadap insiden keselamatan.
b) Prosedur hendaklah meliputi tindakan-tindakan seperti berikut:

i. menganalisis dan mengenal pasti punca kejadian;
ii. merancang dan melaksanakan baik pulih untuk mengelak kejadian daripada berulang, jika perlu;
iii. mengumpul jejak audit dan bukti berkaitan;
iv. berbincang dengan pihak yang menerima akibat daripada pelanggaran insiden keselamatan atau terbabit dengan pemulihan kejadian; dan
v. melapor tindakan yang telah diambil kepada pihak yang berkenaan.

c) Jejak audit yang sesuai dan bukti berkaitan hendaklah dikumpul dan disimpan untuk:

i. analisis masalah dalaman; dan
ii. digunakan sebagai bukti berhubung pelanggaran kontrak, pelanggaran keperluan kawal selia atau sekiranya berlaku prosiding sivil atau jenayah (contoh: penyalahgunaan komputer dan undang-undang perlindungan data).

d) Tindakan untuk memulih insiden keselamatan hendaklah dikawal dengan teliti dan secara formal. Prosedur berikut perlu supaya:

i. individu yang dibenarkan sahaja boleh mencapai sistem dan data secara langsung;
ii. semua tindakan kecemasan yang diambil didokumentasikan dengan sempurna;
iii. tindakan kecemasan hendaklah dilapor kepada pihak pengurusan disemak semula dengan teliti.

e) Keseriusan insiden akan menjadi faktor dalam menentukan saluran penyelesaian masalah.

7.3.2 Jenis-Jenis Insiden Keselamatan

a) Menurut **Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (TMK) (Pekeliling Am Bil. 1 Tahun 2001),** setiap agensi kerajaan dikehendaki melaporkan sebarang insiden keselamatan kepada *Government Computer Emergency Response Team* (GCERT). Laporan insiden keselamatan penting bagi GCERT supaya sokongan teknikal dapat diberikan kepada agensi itu dengan segera (jika dianggap perlu untuk meminimumkan risiko daripada kejadian sedemikian.

b) Jenis insiden keselamatan berikut mestilah dilaporkan kepada GCERT:

i. *Probing*
ii. Serangan *malicious code*
iii. Sangkalan perkhidmatan *(Denial of Service - DoS)*
iv. Capaian tanpa kebenaran
v. Pengubahsuaian perkakasan, perisian atau apa-apa komponen sistem tanpa pengetahuan, arahan atau kelulusan pihak yang berkenaan.

7.3.3 Aras-aras Kritikal

Insiden keselamatan diberi keutamaan berdasarkan aras kritikal:

a) Keutamaan 1

Aktiviti yang boleh mengancam nyawa, keamanan dan keselamatan negara.

b) Keutamaan 2

i. Menceroboh masuk atau cuba menceroboh masuk melalui internet ke dalam *Domain Name Server (DNS), network access point* atau pangkalan data.
ii. Sangkalan perkhidmatan (DoS) yang tersebar.
iii. Menggodam atau mendedahkan sistem kepada ancaman.
iv. Mengganggu sistem tanpa kebenaran.
v. Perbuatan lain (contoh: memalsukan identiti, menukar perisian, laman web atau apa-apa komponen sistem tanpa kebenaran).

c) Keutamaan 3

Pencerobohan hanya menjejaskan sebahagian infrastruktur TMK dan tidak ada tandatanda pencerobohan seterusnya. Sebagai contoh, jangkitan virus terhadap beberapa komputer.

7.4 Prosedur

7.4.1 Melaporkan Insiden Keselamatan

a) Semua insiden keselamatan mestilah disahkan oleh Pentadbir TMK sebaik sahaja insiden itu dikenal pasti.
b) Memaklumkan kepada CIO dan ketua jabatan selepas insiden disahkan.
c) Bergantung pada **Keutamaan** (rujuk **7.3.3. Aras-Aras Kritikal**), insiden mestilah dilaporkan kepada Meja Bantuan yang berkenaan.
d) Melaporkan kepada GCERT jika Meja Bantuan yang berkenaan tidak dapat dihubungi.
e) Sila rujuk **Lampiran E - Maklumat Pihak Bertanggungjawab Bagi Pengendalian Insiden.**

7.4.2 Agihan Tindakan (Escalation Procedures)

Aras Kritikal Insiden	Prosedur Agihan Tindakan
Keutamaan 1	• Mengesahkan insiden. • Memaklumkan kepada Pengurusan Tertinggi Universiti melalui CIO. • Melaporkan kepada Meja Bantuan.
Keutamaan 2	• Mengesahkan insiden. • Memaklumkan kepada CIO • Melaporkan kepada Meja Bantuan.
Keutamaan 3	• Mengesahkan insiden. • Memaklumkan kepada Bahagian Keselamatan TMK PPKT. • Melaporkan kepada Meja Bantuan

7.4.3 Pengumpulan Bukti

Pentadbir TMK hendaklah merekod semua insiden keselamatan yang dikesan. Sekurang-kurangnya, maklumat berikut hendaklah direkod:

a) Tarikh dan masa insiden.
b) Menyenaraikan sistem yang terjejas akibat insiden atau kejadian tersebut.
c) Ringkasan insiden.
d) Tindakan yang diambil untuk membetulkan insiden.
e) Senarai bukti yang diperoleh semasa siasatan.
f) Pengajaran yang diperoleh.

8 Kawalan Perubahan *(Change Control)*

8.1 Pengenalan

Kawalan Perubahan boleh ditafsirkan sebagai proses yang diwujudkan untuk mengurus dan mengawal perubahan yang memberi kesan kepada operasi TMK atau persekitarannya.

8.2 Tujuan

Topik ini bertujuan memastikan proses pertukaran serta peralihan sistem berjalan lancar dan meminimumkan gangguan operasi.

8.3 Garis Panduan

8.3.1 Sebab-sebab Perubahan

Permohonan untuk perubahan disebabkan oleh:

a) ketidakpuasan hati pengguna;
b) keperluan untuk menyelesaikan sesuatu insiden atau masalah;
c) peningkatan keupayaan yang dicadangkan bagi beberapa komponen infrastruktur;
d) perubahan keperluan atau hala tuju; dan
e) perubahan produk atau perkhidmatan daripada penjual atau vendor.

8.3.2 Jenis-jenis Perubahan

Permohonan perubahan boleh meliputi mana-mana bahagian infrastruktur, perkhidmatan atau aktiviti. Sebagai contoh:

a) perkakasan;
b) perisian;
c) kemudahan telekomunikasi; dan
d) dokumentasi.

8.3.3 Proses Kawalan Perubahan

Kawalan perubahan hendaklah mengikut prosedur seperti berikut:

a) membuat permohonan perubahan secara formal;
b) melaksanakan proses pengesahan secara formal;
c) melaksanakan prosedur ujian dan penerimaan sistem bagi setiap perubahan yang mengandungi sekurang-kurangnya ujian unit, ujian komponen dan ujian kesepaduan;
d) mendokumentasikan semua perubahan dan hasil yang dijangkakan;
e) membuat semakan *anti-malicious code* sebelum dan selepas perubahan jika perlu;
f) melaksanakan prosedur *backup* dan penstoran semula *(restore)* untuk mendapatkan imej sistem sebelum mewujudkan persekitaran baru; dan
g) memberi penjelasan untuk meyakinkan pengguna

8.3.4 Maklumat yang Diperoleh

a) Maklumat berikut hendaklah dimasukkan ke dalam Borang Permohonan Perubahan (lihat **Lampiran D - Contoh Borang Permohonan Perubahan):**
   i. Nombor rujukan permohonan perubahan.
   ii. Butiran item yang hendak ditukar.
   iii. Sebab-sebab perubahan.
   iv. Kesan sekiranya tidak melaksanakan perubahan.
   v. Nama, lokasi, nombor telefon pihak/individu yang mencadangkan perubahan tersebut.
   vi. Tarikh dan perubahan yang dicadangkan.
   vii. Keutamaan perubahan.
   viii. Penilaian kesan dan sumber.
   ix. Syor daripada jawatankuasa semakan semula perubahan jika berkaitan.
   x. Tandatangan pihak/individu yang diberi kuasa meluluskan permohonan perubahan.
   xi. Jadual pelaksanaan.

xii. Pelan backup.

xiii. Semakan semula data dan hasil.

b) Pentadbir TMK bertanggungjawab memastikan semua rekod berkaitan difailkan dengan sempurna.

c) Pentadbir TMK juga bertanggungjawab memastikan semua dokumen berkaitan dikemas kini selepas perubahan (contoh: gambar rajah rangkaian).

9 Pelaksanaan Anti-Malicious Code

9.1 Pengenalan

Malicious code seperti virus, *spyware, spam* dan *worm* boleh menjangkiti sistem TMK melalui pelbagai kaedah, termasuk e-mel, internet dan capaian fail yang dijangkiti virus dari *thumb drive,* cakera liut dan CD. *Malicious code* boleh tersebar dengan cepat ke komputer lain dalam rangkaian.

Mesin yang disambungkan ke rangkaian mestilah mempunyai *anti-malicious code* yang sentiasa dikemaskini. *Malicious code* juga boleh menyerang sistem pengoperasian (OS) dan program aplikasi. *Anti-malicious code* mestilah dikemaskini dan dipasang dengan fail tampalan kritikal.

Pentadbir sistem mestilah mengguna pakai sistem perlindungan *anti-malicious code* untuk melawan *malicious code* pada *gateway* e-mel, server dan peranti komputer peribadi.

9.2 Tujuan

Topik ini bertujuan membantu Pentadbir TMK menghalang *malicious code* daripada menyerang/menjangkiti komputer dalam rangkaian dan meminimumkan penyebaran jangkitan.

9.3 Garis Panduan

9.3.1 Pemasangan Perisian *Anti-Malicious Code*

a) Semua mesin, sama ada server, peranti mudah alih (contoh: komputer riba), atau komputer meja hendaklah dipasang dengan *anti-malicious code*. *Anti-malicious code* hendaklah dipasang walaupun mesin itu tidak boleh digunakan untuk mengakses e-mel kerana *malicious code* boleh terus berada dalam fail tanpa dikesan.

b) *Anti-malicious code* pada komputer pengguna hendaklah dikonfigurasikan untuk:

i. memuat turun fail definisi *malicious code* terkini dari server setiap hari;

ii. beroperasi setiap masa, di belakang tabir, automatik, *auto-protect* atau seumpamanya;

iii. mengaktifkan imbasan ingatan, *master records* dan *boot records*, serta fail sistem semasa memulakan mesin; dan

iv. mengimbas semua fail – *Malicious codes* boleh wujud dalam semua jenis fail dan tidak memadai dengan hanya mengimbas program boleh laksana *(executable programmes).*

9.3.2 Konfigurasi Lain

a) Jangan biarkan apa-apa *scripting host* dijalankan pada mesin yang tidak memerlukannya. Kebanyakan *malicious code* ditulis berasaskan *scripting host. Malicious code* tidak boleh beroperasi sekiranya apabila *scripting host* tidak diaktifkan.

b) Mengaktifkan Perlindungan Virus Makro.

c) Nyahaktif paparan tetingkap previu *(preview pane view)* dalam program e-mel. Beberapa *malicious code* boleh dimulakan menerusi paparan previu walaupun mesej itu tidak dibuka.

d) Jangan aktifkan *JavaScript* untuk e-mel.

e) Jangan benarkan lampiran dibuka secara automatik dalam program e-mel.

f) Program e-mel perlu dikonfigurasi untuk memaparkan mesej dalam bentuk teks biasa sahaja. E-mel berformat HTML dikesan mengandungi beberapa kelemahan.

g) Ciri-ciri keselamatan yang terdapat dalam produk perlu digunakan, termasuk menghalang pengguna biasa daripada membuat perubahan dalam program.

9.3.3 Kawalan Integriti Data

a) Jangan benarkan pengguna memasang perisian mesej segera *(instant messaging)*, sembang, dan perisian setara *(peer-to-peer software).*

b) Jangan benarkan pemasangan perisian percuma *(freeware)*, perisian kongsi *(shareware)* atau perisian tanpa kebenaran *(unauthorised software).*

c) Imbas semua program perisian atau fail tampalan *(patches)* sebelum dipasang.

d) Imbas semua media storan boleh alih sebelum diguna.

e) Semak Program Tamat dan Huni Tetap *(Terminate and Stay Resident Programmes*-TSRs) dan Program Huni Ingatan *(Memory Resident Programmes* - MRPs) yang dimuatkan secara automatik sama ada terdapat tanda-tanda diubah atau mempunyai *malicious code.*

9.3.4 Kesedaran Keselamatan

a) Mendidik semua pengguna tentang bahaya kepilan e-mel, *malicious code*, penipuan dan cara membezakan antara ancaman sebenar dengan palsu.

b) Mendidik pengguna tentang program *antimalicious code* yang digunakan dan bagaimana kod ini berfungsi. Hal ini membantu menghapuskan kekeliruan agar pengguna tidak akan melumpuhkan program *anti-malicious code* pada komputer mereka.

9.3.5 Menangani Masalah *Malicious Code*

a) Menentukan jenis dan sumber jangkitan.

b) Melaksana tindakan yang perlu untuk meminimumkan jangkitan *malicious code.*

9.4 Prosedur

9.4.1 Respon Terhadap Masalah *Malicious Code*

a) Pentadbir TMK dinasihati mengenal pasti jenis jangkitan dengan mengemaskini fail definisi *anti-malicious code* pada setiap masa supaya dapat mengenal pasti *malicious code* yang telah memasuki sistem.

b) Semua mesin dalam rangkaian hendaklah diimbas untuk mengenal pasti mesin yang dijangkiti bagi mengesan sumber jangkitan.

c) Semua mesin yang dijangkiti perlu diasingkan untuk mengelakkan jangkitan daripada merebak dengan memutuskan sambungan mesin secara fizikal daripada rangkaian. Sekiranya jangkitan menular, Pentadbir TMK hendaklah menimbang sama ada untuk memutuskan atau tidak keseluruhan rangkaian kerana *malicious code* mungkin menjejaskan rangkaian lain di dalam atau di luar universiti.

d) Program *anti-malicious code* perlu dilaksanakan pada semua mesin yang dijangkiti bagi menghapuskan atau memulihkan jangkitan. Semua mesin mestilah dipulihkan secara manual sama ada dengan menukar konfigurasi *registry* atau membaik pulih atau memasang semula sistem pengoperasian (OS) sekiranya *anti-malicious code* yang dipasang tidak dapat memulihkan jangkitan. Laman web vendor bagi *anti-malicious code* biasanya mengandungi arahan menghapuskan jangkitan secara khusus.

e) Mesin atau rangkaian tidak boleh dihubungkan ke dalam talian sehingga semua kesan *malicious code* dihapuskan. Hal ini memerlukan Pentadbir TMK melakukan imbasan kepada semua mesin sekali lagi.

f) Sekiranya Pentadbir TMK tidak dapat mengawal jangkitan *malicious code*, maka Pentadbir TMK hendaklah melaporkan insiden ini kepada Meja Bantuan dan GCERT.

g) Jangkitan *malicious code* dianggap sebagai insiden keselamatan yang perlu direkod dan ditangani berdasarkan Prosedur Melaporkan Insiden Keselamatan **(Perkara 7.4).**

10 Keselamatan Fizikal Infrastruktur TMK

10.1 Pengenalan

Keselamatan fizikal ialah lapisan pertahanan pertama dalam seni bina keselamatan TMK. Keperluan untuk melindungi aset secara fizikal daripada ancaman sebenar atau yang dijangka tidak boleh diabaikan atau dikesampingkan kerana tidak ada pengganti bagi kawalan keselamatan fizikal yang baik.

10.2 Tujuan

Topik ini bertujuan membantu Pentadbir TMK menghalang capaian tanpa kebenaran, kerosakan dan gangguan kepada infrastruktur fizikal TMK seperti server yang memungkinkan kerosakan atau kemusnahan aset maklumat universiti.

10.3 Garis Panduan

10.3.1 Kawalan Akses Fizikal

a) Sempadan keselamatan hendaklah ditentukan secara jelas dengan akses terkawal, seperti memasang jeriji besi atau menggunakan sistem kad akses.
b) Akses ke makmal komputer dan bilik server hanya dihadkan kepada orang yang dibenarkan.

10.3.2 Perlindungan Kemudahan dan Keselamatan Bilik

a) Bilik server tidak boleh ditempatkan di tingkat bawah bagi mengelak ancaman bencana alam seperti banjir. Bilik server juga tidak boleh ditempatkan di tingkat paling atas yang mungkin mengalami kebocoran.
b) Pintu dan tingkap hendaklah dikunci apabila tidak ada pengguna. Perlindungan keselamatan tambahan hendaklah diambil kira bagi tingkap, khususnya di tingkat bawah.
c) Sistem pengesan pencerobohan yang sesuai hendaklah dipasang dan sentiasa diuji. Sistem pengesan pencerobohan hendaklah meliputi semua pintu luar dan tingkap

yang boleh dimasuki. Kawasan berisiko tinggi seperti bilik server hendaklah dipasang sistem tersebut sepanjang masa.

d) Kelengkapan kawalan hendaklah dipasang untuk meminimumkan risiko ancaman seperti kebakaran. Sebagai contoh memasang sistem penghadang kebakaran, pengesan asap, penangkap kilat atau alat pemadam api.

e) Kawalan hendaklah dijalankan untuk mengurangkan risiko ancaman yang mungkin berlaku seperti suhu melampau. Sebagai contoh, memasang pendingin hawa dan sistem pengudaraan. Pendingin hawa di dalam bilik server hendaklah dipasang pada setiap masa.

f) Bahan berbahaya dan mudah terbakar (contoh: bekalan secara pukal seperti alat tulis dan kotak kosong) tidak boleh disimpan di dalam bilik server.

g) Pentadbir TMK hendaklah memeriksa keselamatan fizikal infrastruktur TMK setiap enam (6) bulan.

h) Pelan laluan kecemasan hendaklah dipamer di tempat yang strategik.

10.3.3 Keselamatan Peralatan

a) Semua kelengkapan mestilah direkod.

b) Bekalan kuasa hendaklah stabil dan bebas daripada gangguan.

c) Kawalan hendaklah dilaksana bagi meminimumkan ancaman yang mungkin berlaku seperti kegagalan bekalan kuasa. Sebagai contoh, menggunakan alat Bekalan Kuasa Tanpa Gangguan (UPS).

d) Peralatan rangkaian perlu disimpan di rak yang sesuai dan dikunci sepanjang masa.

e) Semua anak kunci (contoh: anak kunci rak atau bilik) hendaklah disimpan dengan baik, dibuat pendua dan dilabel. Satu set anak kunci hendaklah disimpan oleh Pentadbir TMK dan satu set yang lain pula hendaklah disimpan di pejabat CIO.

f) Peralatan seperti kabel, server dan komputer hendaklah dipasang dengan betul dan kemas serta dilabel dengan jelas.

g) Kabel hendaklah dilindungi secara fizikal daripada kerosakan sama ada disengajakan atau tidak disengajakan.

h) Semua kabel elektrik tidak boleh diletakkan di atas lantai.

i) Peralatan hendaklah diletakkan di tempat yang sesuai. Sebagai contoh, server tidak boleh diletakkan tepat di bawah pendingin hawa.

j) Peralatan TMK hendaklah dilindungi daripada disambar kilat dengan memasang penangkap kilat dan pelindung pusuan kuasa *(power surge protector).*

k) Pemindahan peranti mudah alih seperti komputer bimbit, projektor LCD dan *tablet PCs* mestilah mendapat kebenaran terlebih dahulu, direkod dan dipantau.

10.3.4 Pengendalian Pelawat

a) Kehadiran pelawat di makmal komputer dan bilik server hendaklah direkodkan di dalam buku log. Rekod hendaklah mengandungi nama, tarikh, masa dan tujuan memasuki tempat tersebut.

b) Kehadiran pelawat di makmal komputer dan bilik server hendaklah diiringi oleh kakitangan yang dibenarkan. Pelawat hanya dibenarkan masuk untuk tujuan tertentu. Jika perlu, pelawat hendaklah diberi taklimat tentang keselamatan kawasan tersebut dan prosedur kecemasan.

c) Aktiviti yang dilakukan di dalam bilik server dan makmal komputer hendaklah diawasi atas sebab-sebab keselamatan bagi mengelak berlakunya perkara yang tidak diingini.

11 Lampiran A : Senarai Semakan Semula Pematuhan

Pusat Tanggungjawab :	
Kawasan Teknikal :	
Nama Respondan :	

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
1. Keselamatan	1. Adakah akses ke kawasan berisiko tinggi seperti bilik server, makmal komputer dikawal dan dihadkan kepada individu yang dibenarkan?				
	2. Adakah bilik server dan makmal komputer dipasang jeriji besi dan dikunci apabila tidak digunakan?				
	3. Adakah kehadiran pelawat di kawasan berisiko tinggi direkodkan dan diselia?				
	4. Adakah sistem pendingin hawa dan pengudaraan disediakan?				
	5. Adakah pendingin hawa diletakkan tepat di atas server?				
	6. Adakah alat pemadam api dan pencegah kebakaran dipasang dan berfungsi?				
	7. Adakah alat bekalan kuasa tanpa gangguan (UPS) atau penjana kuasa disediakan?				
	8. Adakah mesin diletakkan di tempat yang sesuai untuk mengelakkan bencana alam seperti banjir dan kebocoran?				
	9. Adakah kelengkapan ICT (server/komputer) dan kabel dilabel dengan betul?				

Lampiran A

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
	10. Adakah kabel dipasang dengan teratur?				
	11. Adakah kelengkapan ICT diselenggara secara berkala?				
2. Backup	1. Adakah media *backup* diwujudkan seperti yang ditetapkan dan sentiasa dikitar serta ditempatkan di luar kawasan untuk mengelakkan gangguan jika fail semasa rosak?				
	2. Adakah terdapat manual terperinci untuk memulihkan operasi?				
	3. Adakah dokumen sistem dan aplikasi disimpan di luar kawasan?				
	4. Adakah lokasi penyimpanan *backup* dikenal pasti?				
	5. Adakah lokasi di luar kawasan dilindungi secara fizikal?				
	6. Adakah penstoran semula dan pengujian dilakukan sekurang-kurangnya sekali setahun?				
3. Kesedaran Keselamatan	1. Adakah program kesedaran keselamatan dilaksanakan?				
	2. Adakah pengguna menerima salinan, atau dibenarkan untuk mengakses garis panduan dan prosedur keselamatan yang berkenaan?				
4. Keupayaan Pengendalian Insiden	1. Adakah insiden keselamatan, kelemahan atau kegagalan fungsi sistem dilaporkan?				
	2. Adakah insiden direkodkan dan dipantau?				

Lampiran A

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
5. Penyelenggaraan Sistem	1. Adakah proses pengurusan perubahan dipatuhi apabila Sistem sebarang perubahan dibuat kepada server?				
	2. Adakah sistem sentiasa dipantau dan dikemas kini apabila terdapat fail kemas kini *(updates)* dan fail tampalan *(patches)* terkini?				
6. Pemantauan	1. Adakah jejak audit dan log diperiksa mengikut jadual yang ditetapkan oleh pihak yang bertanggungjawab?				
	2. Adakah log disemak kaji semula dan dipantau?				
7. Pengurusan Capaian Pengguna	1. Adakah ID pengguna bertepatan dengan konvensi nama?				
	2. Adakah tahap capaian diberikan sejajar dengan fungsi kerja?				
	3. Adakah akaun pengguna digantung/dihapus selepas pengguna meletak jawatan, menamatkan pengajian atau bertukar kerja?.				
	4. Adakah capaian pengguna disekat setelah gagal log masuk tiga (3) kali berturut-turut?				
8. Pengurusan Kata Laluan	1. Adakah pengguna dipaksa menukar kata laluan apabila log masuk kali pertama dengan kata laluan yang baru?				
	2. Adakah kata laluan pengguna perlu ditukar setiap 180 hari?				
	3. Adakah kata laluan mempunyai sekurang-kurangnya lapan (8) aksara yang terdiri daripada alphanumerik				

	dan simbol?				
	4. Adakah pengguna dibenarkan mengguna semula empat (4) kata laluan yang terdahulu?				
	5. Adakah kata laluan dipaparkan sebagai teks jelas pada skrin apabila dimasukkan?				
	6. Adakah kata laluan di server disimpan dalam bentuk teks jelas?				
9. Anti-Malicious Code	1. Adakah semua komputer meja dan peranti mudah alih (contohnya komputer riba) dipasang dengan *anti-malicious code?*				
	2. Adakah fail definisi *anti-malicious code* dikemas kini secara berkala untuk server, komputer meja atau peranti mudah alih?				

Saya mengaku bahawa semua maklumat yang diberikan dalam dokumen ini adalah betul dan benar sepanjang pengetahuan dan pemahaman saya.

Tandatangan : .....

Nama : .....

Tarikh : .....

12 Lampiran B – Contoh Notis bagi Penyalahgunaan Sumber TMK

NOTIS PEMBERITAHUAN

Kepada : Ketua Pegawai Maklumat Tarikh : <Tarikh>

Daripada : <Pentadbir TMK>

Perkara : **Penyalahgunaan Kemudahan TMK Universiti Sains Malaysia**

Secara umumnya kemudahan sistem komunikasi elektronik atau TMK Universiti Sains Malaysia digunakan untuk operasi harian.

Kemudahan ini tidak boleh digunakan untuk kegiatan jenayah atau peribadi yang mungkin menimbulkan gangguan seks, perkauman atau bangsa. Penggunaan kemudahan ini sentiasa dipantau oleh Pentadbir TMK untuk memastikan penggunaannya bersesuaian seperti yang ditetapkan dalam buku **Garis Panduan dan Prosedur Pengurusan Keselamatan Teknologi Maklumat Dan Komunikasi (TMK) Universiti Sains Malaysia untuk Pentadbir TMK.**

Pengguna berikut dikenal pasti telah melanggar Garis Panduan dan Prosedur Pengurusan Keselamatan TMK.

Nama & Nombor Matrik/Staf :
Jawatan/ Pusat Pengajian /
Jabatan:
Butiran pelanggaran garis
panduan keselamatan:

Untuk menangani pelanggaran tersebut, adalah disyorkan supaya tindakan berikut diambil mengikut keseriusan pelanggaran tersebut.

- ❑ Membincangkan isu itu dengan individu tersebut.
- ❑ Menerangkan kepentingan memahami Garis Panduan dan Prosedur tersebut.
- ❑ Bagi kejadian pertama, amaran lisan diberikan dan tentukan sama ada amaran bertulis diperlukan atau tidak.
- ❑ Bagi kejadian kedua dan seterusnya, tentukan tindakan yang perlu diambil.

Sekiranya pihak tuan/puan memerlukan penjelasan lanjut tentang insiden kejadian tersebut, sila hubungi saya.

————————————————

(Tandatangan)

Lampiran C

13 Lampiran C – Contoh Penilaian Program Kesedaran

Tajuk :

Pembentang :

Tarikh :

Nama :

Jawatan/Tahun & Bidang Pengajian

Tandakan (✓) di mana berkenaan.

(A) Penilaian Kesedaran Secara Keseluruhan	**4**	**3**	**2**	**1**	**0**
1. Penilaian secara keseluruhan					
2. Kualiti grafik					
3. Kualiti kelengkapan audio/visual					
4. Kandungan penyampaian					

	Cepat		Sederhana		Lambat
	4	**3**	**2**	**1**	**0**
5. Kelancaran penyampaian secara umum					

(B) Ulasan tentang penyampaian

(C) Aspek manakah yang paling anda sukai dalam program tersebut?

(D) Bagaimanakah program kesedaran ini boleh ditambah baik?

---

14 Lampiran D – Contoh Borang Permohonan Perubahan

Borang Permohonan Perubahan

No. Ruj :

Butiran Pemohon

Nama:	Jawatan	No. Tel: Samb :

Butiran Perubahan

Keterangan :

Sebab-Sebab :

Tempoh Masa

Lampiran *(Tandakan (✓) di mana berkenaan)*

❑ Pelan pelaksanaan

❑ Pelan pengujian

❑ Pelan maklum balas

Keutamaan

(Tandakan (✓) di mana berkenaan)

❑ Segera

❑ Keutamaan biasa

Kesan Perubahan

(Tandakan (✓) di mana berkenaan)

❑ Major

❑ Minor

Diluluskan oleh,

.....

Nama :

No. Telefon & Sambungan :

Tarikh :

Perubahan yang dicadangkan di atas:

❑ Berjaya dilaksanakan pada : _____

❑ Tidak berjaya kerana: _____

Disemak oleh,

.....

Nama :

No. Telefon & Sambungan :

Tarikh :

15 Lampiran E – Maklumat Pihak Bertanggungjawab Bagi Pengendalian Insiden

a) Meja Bantuan

Servisdesk@PPKT

Pusat Perkhidmatan Komunikasi & Teknologi

Universiti Sains Malaysia

No. Tel. :

No. Faks :

E-mel : servisdesk@usm.my

b) GCERT

Pasukan Petugas Khas Kecemasan Komputer Kerajaan (GCERT)

Bahagian Keselamatan TMK, MAMPU

Aras 5, Blok B1

Kompleks Jabatan Perdana Menteri

Pusat Pentadbiran Kerajaan Persekutuan

62502 Putrajaya

No. Tel. : 03-8888 3150

No. Faks : 03-8888 3286

E-mel : gcert@mampu.gov.my

Melaporkan insiden keselamatan di luar waktu pejabat

Jika insiden keselamatan adalah kritikal dan boleh membahayakan nyawa, keselamatan diri atau negara, GCERT boleh dihubungi di nombor berikut:

Ketua Pegawai Maklumat Universiti Sains Malaysia

No Telefon : 03-8888 2250

atau

Pegawai Keselamatan Teknologi Maklumat

No Telefon :

16 GLOSARI

Sangkalan Perkhidmatan *(Denial of Service)*	Satu serangan yang menghalang atau (DoS) merosakkan penggunaan rangkaian, sistem atau penggunaan yang dibenarkan dengan menghabiskan sumber.
Perisian Percuma *(Freeware)*	Perisian yang mempunyai hak cipta yang diberikan percuma oleh penulisnya.
Penggodam *(Hackers)*	Individu yang melakukan capaian tanpa kebenaran ke dalam sistem komputer bagi tujuan mencuri dan/atau merosakkan data
Penceroboh *(Intruder)*	Seseorang yang mencapai rangkaian, sistem, aplikasi, data atau sumber lain tanpa kebenaran.
Kegagalan fungsi (*Malfunction)*	Ketidakupayaan sistem untuk beroperasi seperti biasa.
Malicious Code	Kod yang dimuatkan ke dalam komputer tanpa pengetahuan dan kebenaran pemilik, khusus untuk merosakkan atau melumpuhkan sistem seperti virus, *worm* atau *Trojan Horse.*
Peer-to-peer	Sejenis rangkaian yang setiap stesen kerja mempunyai keupayaan dan tanggungjawab yang sama.
Probing	Pengintipan ke dalam sistem atau data.
Risiko *(Risk)*	Secara umumnya, kemungkinan menghadapi bahaya atau mengalami kerosakan atau kehilangan, terutamanya kerana kurang berhati-hati.
Insiden Keselamatan *(Security Incident)*	Perlakuan atau ancaman yang mungkin melanggar dasar keselamatan TMK.
Kelemahan Keselamatan	Ciri atau unsur yang boleh diketahui *(Security Weakness)* kuantitinya dan bebas ancaman bagi aset dalam persekitaran sistem operasi, dan mungkin meningkatkan kejadian ancaman yang menyebabkan kerosakan dari segi kerahsiaan, ketersediaan atau integritinya, atau meningkatkan kesan sesuatu kejadian ancaman jika berlaku.
Bilik Server *(Server Room)*	Bilik yang menempatkan komputer / server yang membolehkan perkongsian sumber seperti pencetak dan fail.
Perisian Kongsi *(Shareware)*	Perisian percuma yang boleh dicuba untuk tempoh tertentu sebelum dibeli sepenuhnya.
Spyware	Mana-mana perisian yang secara tersembunyi mengumpulkan maklumat pengguna melalui sambungan internet pengguna tanpa pengetahuannya, biasanya bagi tujuan iklan.
Ancaman *(Threat)*	Sebarang kejadian atau tindakan yang mungkin boleh mendatangkan bahaya atau menyebabkan berlakunya perkara-perkara seperti pendedahan tanpa izin, kerosakan, penyingkiran, pengubahsuaian atau gangguan maklumat, aset atau perkhidmatan yang sensitif atau kritikal. Ancaman boleh berlaku secara biasa,dengan sengaja atau tidak sengaja.

17 Rujukan

1) Buku Panduan Keselamatan Pengurusan Teknologi Maklumat & Komunikasi Sektor Awam Malaysia (MyMIS), 2002.
2) Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (TMK) (Pekeliling Am Bil. 1 Tahun 2001).
3) Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan (Pekeliling Am Bil. 3 Tahun 2000).

Pertanyaan

Pertanyaan tentang dokumen ini hendaklah ditujukan kepada:

Ketua Pegawai Maklumat

Universiti Sains Malaysia

Minden

11800 Pulalu Pinang

Tel.:

Faks:

E-mel: