UNIVERSITI SAINS MALAYSIA

PPKT enovate Pusat Pengetahuan, Komunikasi & Teknologi

GARIS PANDUAN

Keselamatan Teknologi Maklumat dan Komunikasi

Pusat Pengetahuan, Komunikasi Dan Teknologi
Universiti Sains Malaysia

enovate.usm.my

ISMS SIRIM
IQNet CERTIFIED MANAGEMENT SYSTEM
CERTIFIED TO ISO/IEC 27001:2013
CERT. NO : ISMS 00314

Tajuk Dokumen	:	GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI UNIVERSITI SAINS MALAYSIA
No. Terbitan	:	3.1
Tarikh Kuatkuasa	:	18 APRIL 2023

GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

Kandungan

Kandungan ii

Definisi vii

1 Pendahuluan 1

1.1 Pengenalan 1

1.2 Tujuan 1

1.3 Tanggungjawab 2

1.4 Struktur Garis Panduan 3

2 Pengurusan Capaian Pengguna 5

2.1 Pengenalan 5

2.2 Tujuan 5

2.3 Garis Panduan 5

2.3.1 Pendaftaran/Pembatalan Akaun Pengguna 5

2.3.2 Pengurusan Peranan dan Hak Capaian *(Privilege Management)* 6

2.3.3 Penyelenggaraan Akaun Pengguna 6

2.3.4 Pengurusan Kata Laluan Pengguna 7

2.3.5 Semakan Semula Hak Capaian Pengguna 8

2.3.6 Pelaksanaan Kawalan Capaian 8

2.3.7 Pelaksanaan Polisi Kumpulan *(Group Policy)* 9

2.3.8 Pelaksanaan Kriptografi 9

2.3.9 Meja Bersih (*Clear Desk*) Dan Skrin Bersih (*Clear Screen*) 9

3 Sandaran (*Backup*) dan Pemulihan *(Restore)* 11

3.1 Pengenalan 11

3.2 Tujuan 11

3.3 Garis Panduan 11

3.3.1 Penstoran Media Sandaran di Luar Kawasan *(Offsite Backup)* 11

3.3.2 Pengujian Media Sandaran 11

3.3.3 Penyemakan Prosedur Pemulihan 12
3.3.4 Jadual Sandaran 12
3.3.5 Kitaran Media dan Tempoh Penyimpanan 12
3.3.6 Pelabelan dan Penamaan Media 12
4 Semakan Semula Pematuhan *(Compliance Review)* 13
4.1 Pengenalan 13
4.2 Tujuan 13
4.3 Garis Panduan 13
4.3.1 Semakan Semula Pematuhan Secara Berkala 13
4.3.2 Proses Kajian Semakan Semula 14
5 Pemantauan Keselamatan *(Security Monitoring)* 15
5.1 Pengenalan 15
5.2 Tujuan 15
5.3 Garis Panduan 15
5.3.1 Bidang Pemantauan Keselamatan 15
5.3.2 Respon kepada Salah Guna 16
5.3.3 Respon kepada Insiden Keselamatan yang Berpotensi 17
6 Kesedaran Keselamatan *(Security Awareness)* 19
6.1 Pengenalan 19
6.2 Tujuan 19
6.3 Garis Panduan 19
6.3.1 Merancang Program Kesedaran Keselamatan 19
6.3.2 Kekerapan Program Kesedaran Keselamatan 20
6.3.3 Komponen Program Kesedaran Keselamatan 20
7 Pengendalian Insiden Keselamatan TMK *(ICT Security Incident Handling)* 21
7.1 Pengenalan 21
7.2 Tujuan 21

7.3 Garis Panduan 21
7.3.1 Peraturan Am 21
7.3.2 Jenis-Jenis Insiden Keselamatan 22
7.3.3 Aras-aras Kritikal 23
7.4 Prosedur 24
7.4.1 Melaporkan Insiden Keselamatan 24
7.4.2 Pengumpulan Bukti 24
8 Kawalan Perubahan (Change Control) 25
8.1 Pengenalan 25
8.2 Tujuan 25
8.3 Garis Panduan 25
8.3.1 Sebab-sebab Perubahan 25
8.3.2 Jenis-jenis Perubahan 25
8.3.3 Proses Kawalan Perubahan 26
8.3.4 Maklumat yang Diperoleh 26
9 Perlindungan peranti 28
9.1 Pengenalan 28
9.2 Tujuan 28
9.3 Garis Panduan 28
9.3.1 Pemasangan Perisian Anti-Kod Hasad 28
9.3.2 Konfigurasi Lain 29
9.3.3 Kawalan Integriti Data 29
9.3.4 Kesedaran Keselamatan 30
9.3.5 Menangani Masalah Kod Hasad 30
9.4 Prosedur 30
9.4.1 Respon Terhadap Masalah *Malicious Code* 30
10 Keselamatan Fizikal Infrastruktur TMK 32

10.1 Pengenalan 32

10.2 Tujuan 32

10.3 Garis Panduan 32

10.3.1 Kawalan Akses Fizikal 32

10.3.2 Perlindungan Kemudahan dan Keselamatan Bilik Pelayan 32

10.3.3 Keselamatan Peralatan 33

10.3.4 Pengendalian Pelawat 34

10.3.5 Pelupusan Data 34

11 Pertukaran Maklumat 35

11.1 Pengenalan 35

11.2 Tujuan 35

11.3 Garis Panduan 35

11.3.1 Pengurusan Pertukaran Maklumat 35

11.3.2 Pengurusan Mel Elektronik (Emel) 36

11.3.3 Storan Internet 37

12 Pembangunan dan Pengurusan Aplikasi 38

12.1 Pengenalan 38

12.2 Tujuan 38

12.3 Garis Panduan 38

12.3.1 Pembangunan Aplikasi 38

12.3.2 Pengurusan Aplikasi 40

13 Keselamatan Rangkaian dan Telekomunikasi 41

13.1 Pengenalan 41

13.2 Tujuan 41

13.3 Garis Panduan 41

13.3.1 Infrastuktur Rangkaian dan Telekomunikasi 41

14 Penggunaan Peranti Peribadi (*Bring Your Own Device* , BYOD) 44

14.1 Pengenalan 44

14.2 Tujuan 44

14.3 Garis Panduan 44

Lampiran A : Senarai Semakan Semula Pematuhan 46

Lampiran B – Contoh Notis bagi Penyalahgunaan Sumber TMK 50

Lampiran C – Contoh Penilaian Program Kesedaran 51

Lampiran D – Contoh Borang Permohonan Perubahan 52

Lampiran E – Jadual Komponen Program Keselamatan TMK 53

Lampiran F – Maklumat Pihak Bertanggungjawab Bagi Pengendalian Insiden 54

GLOSARI 55

RUJUKAN 57

Definisi

a) Penyedia Perkhidmatan TMK - staf yang menyelia secara langsung infrastruktur dan perkhidmatan TMK di bawah tanggungannya.

b) Pentadbir Keselamatan TMK – Unit atau individu yang dilantik untuk menguruskan dan memantau isu-isu berkaitan keselamatan TMK

c) Pengguna Perkhidmatan TMK – pengguna yang menggunakan perkhidmatan TMK yang ditawarkan di USM.

d) Storan Internet – Tempat simpanan data digital yang boleh dicapai melalui rangkaian internet.

e) Sumber Luar – Sebarang perolehan perkhidmatan atau produk yang bukan dihasilkan oleh warga USM.

f) Rangkaian – Sambungan talian digital dalam beberapa koleksi perkakasan dan peranti untuk perkongsian data digital.

g) USMNet – Talian rangkaian intranet dan internet USM

h) Remote Access – Capaian ke peranti melalui rangkaian luar ke rangkaian dalaman USM

i) Penggunaan Peranti Peribadi (BYOD) - Sebarang peranti IT yang bukan milik USM digunakan di dalam rangkaian USM.

Tajuk Dokumen	:	GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI UNIVERSITI SAINS MALAYSIA
No. Terbitan	:	3.1
Tarikh Kuatkuasa	:	18 APRIL 2023

1 Pendahuluan

1.1 Pengenalan

Pada masa kini institusi semakin bergantung kepada penggunaan sistem automasi 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, maka Pentadbir Keselamatan 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 digunapakai dalam menyokong operasi di universiti, dan tertakluk kepada semakan berkala. USM mempunyai hak untuk mengemaskini dokumen ini apabila perlu.

Prosedur operasi standard akan menerangkan dengan lebih lanjut kaedah perlaksanaan garis panduan yang dinyatakan dalam dokumen ini pada peringkat operasi dan perlaksanaan.

1.2 Tujuan

Tujuan utama buku panduan ini adalah:

a) Menggariskan tanggungjawab Pentadbir Keselamatan TMK terhadap keselamatan TMK.

b) Memberikan garis panduan dan prosedur kepada Pentadbir TMK dan Pentadbir Keselamatan maklumat di USM berdasarkan DTMK dan Perintah Am Kerajaan Malaysia.

c) Menyatakan garis panduan dan prosedur yang perlu dipatuhi oleh penyedia-penyedia perkhidmatan berkaitan TMK kepada USM.

d) Menyatakan garis panduan dan prosedur kepada pengguna-pengguna perkhidmatan berkaitan TMK yang ditawarkan di USM.

1.3 Tanggungjawab

Pentadbir Keselamatan 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 USM 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 berkaitan dengan keselamatan 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.
i) Memastikan semua perisian dan perkakasan yang digunakan serta fail tampalan *(patches)* adalah mengikut keperluan dan berfungsi dengan baik.

Penyedia Perkhidmatan TMK dikehendaki:

a) memahami kandungan buku panduan ini dan mematuhi garis panduan dan prosedur yang telah ditetapkan dalam menyediakan perkhidmatan berkaitan TMK di USM.

Pengguna Perkhidmatan TMK yang disediakan di USM dikehendaki:

a) Memahami kandungan buku panduan ini dah mematuhi garis panduan dan prosedur yang telah ditetapkan dalam menggunakan perkhidmatan berkaitan TMK di USM.

1.4 Struktur Garis Panduan

Struktur garis 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) **Sandaran (*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 Keselamatan 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 Keselamatan TMK dalam penyediaan bilik pelayan.

j) **Pertukaran Maklumat** menetapkan garis panduan dan prosedur mengurus pertukaran maklumat antara pengguna TMK di dalam USM sama ada dengan individu atau agensi luar USM yang melibatkan kerahsiaan maklumat**.**

k) **Pembangunan dan Pengurusan Aplikasi** menetapkan garis panduan dalam pembangunan atau perolehan kepada sesuatu aplikasi dengan mengadaptasi standard pengurusan pembangunan, pengujian, pemasangan dan penyelenggaraan yang baik dan selamat.

l) **Keselamatan Rangkaian dan Telekomunikasi** menetapkan garis panduan keselamatan penggunaan sistem rangkaian dan telekomunikasi USM.

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.

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 Keselamatan 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 identiti yang unik dan kata laluan permulaan. Hal ini untuk memastikan pengguna sendiri bertanggungjawab bagi sebarang aktiviti yang melibatkan penggunaan akaun identiti mereka.

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

c) Kumpulan dan peranan pengguna mestilah ditentukan dan disahkan terlebih dahulu oleh Pentadbir Keselamatan TMK dan penyedia perkhidmatan TMK.

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

e) Pentadbir Keselamatan 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. Akaun identiti pengguna digantung dalam tempoh masa yang sesuai sebelum dihapuskan.

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

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

b) Pentadbir Keselamatan TMK dicadangkan meminimumkan perubahan peranan dan hak capaian bagi setiap kumpulan kecuali diwajarkan mengikut keperluan urusan dan dibenarkan oleh pengarah PPKT atau pihak pengurusan atasan 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 Keselamatan TMK dan pemegang akaun tersebut boleh memainkan peranan sokongan dengan persetujuan Pengarah PPKT.

2.3.3 Penyelenggaraan Akaun Pengguna

a) Pengurusan akaun pengguna terletak di bawah tanggungjawab pengguna. Jika pengguna mempunyai sebarang permasalahan berkenaan akaun, pengguna boleh menghubungi meja bantuan untuk mendapatkan bantuan.

b) Sekiranya peranan pengguna bertukar (disebabkan kenaikan pangkat atau apa-apa sebab lain), Pentadbir Keselamatan TMK perlu mengkaji semula peranan dan hak capaian pengguna untuk mengakses sistem. Mana-mana permohonan pertukaran sedemikian hendaklah dipertimbangkan dengan sewajarnya dan direkodkan.

2.3.4 Pengurusan Kata Laluan Pengguna

a) Peraturan kata laluan berikut mestilah dikuatkuasakan oleh Pentadbir Keselamatan TMK dan memenuhi kompleksiti seperti berikut:

i. Kata laluan perlu sekurang-kurangnya 8 aksara, panjang aksara maksima bergantung kepada keperluan sistem.

ii. Tidak menyerupai nama pengguna, akaun identiti atau maklumat am pengguna seperti nombor plat, tarikh lahir atau nombor telefon.

iii. Mempunyai sekurang-kurangnya 3 kombinasi dari jenis huruf besar, huruf kecil, nombor dan simbol.

iv. Tidak menggunakan kata laluan yang digunakan pada sistem lain, kata laluan yang lemah atau kata laluan yang pernah diceroboh.

i.

b) Bagi mengurangkan risiko ancaman keselamatan:

i. Kata laluan tidak boleh dikongsi dengan pengguna lain.

ii. Setiap akaun identiti pengguna mestilah dipautkan kepada kata laluan yang hanya diketahui oleh pengguna tersebut.

iii. Pengguna digalakkan memperbaharui kata laluan dengan setiap 6 bulan

iv. Pengguna perlu menukarkan kata laluan dengan segera jika mengesyaki kata laluan telah terbocor dan melaporkan insiden tersebut kepada Pentadbir Keselamatan TMK.

2.3.5 Semakan Semula Hak Capaian Pengguna

a) Bagi memastikan kawalan yang berkesan dalam mencapai maklumat dan sistem TMK, Pentadbir Keselamatan TMK perlu memberi cadangan, menasihatkan dan memantau Pentadbir-pentadbir TMK untuk:

i. Mengkaji semula hak capaian secara berkala; dan

ii. Menyemak hak capaian istimewa (misalnya akaun *root* atau *administrator*) secara berkala.

iii. Pentadbir Keselamatan TMK dan Pentadbir-pentadbir TMK yang berkaitan 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.

i. Pengguna akan dilog keluar secara automatik oleh sistem selepas tempoh maksimum yang ditentukan bagi skrin melahu (contohnya 10 minit),

ii. Akaun pengguna akan dihalang sementara apabila gagal proses pengesahan log masuk secara berturut-turut. Bilangan dan masa halangan adalah mengikut kesesuaian sistem dan keadaan semasa.

iii. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan maklumat jika capaian tidak sah.

b) Pentadbir TMK, Pentadbir Keselamatan TMK atau pegawai yang dilantik untuk mengakses maklumat atau servis pengguna atas dasar perlu dengan kebenaran Pengarah PPKT secara bertulis.

2.3.7 Pelaksanaan Polisi Kumpulan *(Group Policy)*

a) Pentadbir Keselamatan TMK hendaklah menentukan polisi bagi kumpulan, pengguna dan mesin untuk mengawal capaian kepada sumber.

b) Semua stesen kerja dan pelayan hendaklah dikonfigurasikan untuk menerima pelbagai polisi pengguna atau unit organisasi (OU).

2.3.8 Pelaksanaan Kriptografi

a) Penghantaran kata laluan melalui aplikasi sesawang perlulah penyulitan (*encrypt*).

b) Kunci peribadi yang digunakan dalam proses kritografi perlu dilindungi dan disimpan dengan selamat.

c) Kunci kriptografi yang telah dikompromi perlu ditukar dengan kunci kritografi yang baru.

d) Sijil digital kriptografi perlu mempunyai tarikh luput dan diperbaharui apabila tempoh sah penggunaan tamat.

e) Protokol-protokol yang menggunakan fungsi kriptografi yang lemah perlu ditukar dengan protokol yang mempunyai fungsian kriptografi yang selamat.

f) Pengguna yang menggunakan servis *Private Key Infrastructure* (*PKI*), perlu bertanggung jawab kepada kunci peribadi sijil digital kriptografi tersebut.

2.3.9 Meja Bersih (*Clear Desk*) Dan Skrin Bersih (*Clear Screen*)

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Meja Bersih* dan *Skrin Bersih* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Mengunci skrin dengan kata laluan atau log keluar apabila meninggalkan komputer.

b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.

c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat

3 Sandaran (*Backup*) dan Pemulihan *(Restore)*

3.1 Pengenalan

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

3.2 Tujuan

Topik ini bertujuan membantu Pentadbir Keselamatan TMK atau Pentadbir TMK melaksanakan proses sandaran, pemulihan dan pelan pemulihan bencana *(disaster recovery)* secara berkesan.

3.3 Garis Panduan

3.3.1 Penstoran Media Sandaran di Luar Kawasan *(Offsite Backup)*

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

   i. Rekod sandaran yang tepat dan lengkap.
   ii. Dokumen prosedur pemulihan.
   iii. Sekurang-kurangnya tiga (3) generasi sandaran.

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

3.3.2 Pengujian Media Sandaran

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

3.3.3 Penyemakan Prosedur Pemulihan

Prosedur Pemulihan hendaklah disemak dan diuji secara berkala untuk memastikan proses pemulihan berkesan dan boleh disempurnakan mengikut masa yang ditetapkan**.**

3.3.4 Jadual Sandaran

a) Sandaran mestilah dilakukan secara berkala mengikut tahap kritikal sesuatu data atau sistem.
b) Sandaran perlu merangkumi keseluruhan sistem, pangkalan data, konfigurasi dan aplikasi yang digunakan.
c) Semua sandaran hendaklah dijadualkan pada luar waktu puncak (misalnya pada waktu malam) atau tempoh yang tidak mengganggu operasi sistem yang disandarkan mengikut keperluan perkhidmatan.

3.3.5 Kitaran Media dan Tempoh Penyimpanan

a) Pentadbir Keselamatan TMK atau pentadbir TMK hendaklah melaksanakan skema kitaran mengikut keperluan perkhidmatan.
b) Media yang mempunyai peratus kerosakan yang tinggi atau kecenderungan untuk gagal perlu dilupuskan dan memastikan maklumat yang terkandung di dalamnya dimusnahkan.

3.3.6 Pelabelan dan Penamaan Media

Setiap media sandaran hendaklah dilabel atau dinamakan dengan sempurna selepas Pentadbir TMK selesai membuat sandaran bagi memastikan media yang betul digunakan untuk tujuan yang dimaksudkan. Label itu mestilah mengandungi identiti, tarikh sandaran dan maklumat lain yang dirasakan perlu.

4 Semakan Semula Pematuhan *(Compliance Review)*

4.1 Pengenalan

Semakan semula pematuhan secara berkala merupakan mekanisme untuk Pentadbir Keselamatan TMK menentukan status program keselamatan TMK. Jika perlu, kelemahan dikenal pasti bagi tujuan penambahbaikan. Proses ini juga menjadi mekanisme bagi USM mengumpul maklum balas tentang keberkesanan program keselamatan sedia ada daripada Pentadbir Keselamatan TMK.

4.2 Tujuan

Topik ini bertujuan memberikan garis panduan kepada Pentadbir Keselamatan TMK untuk:

a) Melakukan semakan semula pematuhan sekurang-kurangnya satu (1) kali setiap tahun.
b) Meningkatkan tahap pemantau bidang kawalan dengan lebih cekap.
c) Mengkaji semula senarai semak pematuhan penilaian kendiri.

4.3 Garis Panduan

4.3.1 Semakan Semula Pematuhan Secara Berkala

a) Pentadbir TMK dan Pentadbir Keselamatan TMK hendaklah melakukan semakan semula pematuhan secara berkala untuk memastikan pelaksanaan kawalan keselamatan TMK mematuhi garis panduan berprosedur yang diberikan oleh dokumen ini.
b) Pentadbir TMK dan Pentadbir Keselamatan 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 dan keperluan Universiti.

4.3.2 Proses Kajian Semakan Semula

a) Kajian semula pematuhan hendaklah berbentuk soal selidik yang perlu dilengkapkan oleh Pentadbir TMK.

b) Pengarah PPKT berhak untuk membenar atau tidak membenar pengecualian pematuhan setelah mengambil kira risiko keselamatan.

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

d) Kajian semula pematuhan mestilah dijalankan pada minimum satu (1) kali setiap dua tahun dan keputusannya hendaklah dimaklumkan kepada Majlis Teknologi Maklumat, Ketua Pegawai Maklumat atau Pengarah PPKT mengikut kesesuaian.

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 dan Pentadbir Keselamatan TMK mengambil langkah proaktif untuk 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 Keselamatan TMK untuk menentukan aktiviti biasa dan luar biasa dalam sistem TMK, jika perlu.
b) Bidang yang patut dipertimbangkan untuk pemantauan termasuklah:

i. Capaian yang dibenarkan, termasuk butiran seperti berikut:
   - Akaun identiti pengguna.
   - Tarikh dan masa peristiwa penting.
   - Jenis peristiwa.

ii. Semua operasi khusus, seperti:
   - Penggunaan akaun pentadbir.
   - Pemula dan penghenti sistem.

- Memasang/menanggal peranti I/O.

iii. Percubaan capaian tanpa kebenaran, seperti:

- Percubaan yang gagal.
- Pelanggaran polisi capaian.
- Amaran daripada *firewall* atau sistem pengesanan pencerobohan atau lain-lain peranti atau perisian keselamatan.

iv. Amaran atau kegagalan sistem, seperti:

- Amaran atau mesej.
- Pengecualian log sistem.

v. Log aplikasi atau peranti

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

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

5.3.2 Respon kepada Salah Guna

Langkah-langkah tindakan hendaklah merujuk kepada dokumen berkaitan perkhidmatan dalam konteks keselamatan TMK.

Dokumen tersebut harus mengandungi maklumat-maklumat berikut mengikut kesesuaian servis:

i. Mengesan nama pengguna yang melanggar tata cara penggunaan aplikasi atau servis.

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. (Rujuk Lampiran B: Contoh Notis Pemberitahuan Bagi Penyalahgunaan Sumber TMK).

vi. Menghantar notis pemberitahuan salah guna kepada kumpulan tindakan, pengarah PPKT, CIO atau badan lain mengikut kesesuaian.

vii. Memberikan butiran terperinci tentang penyalahgunaan jika diminta oleh kumpulan tindakan, pengarah PPKT, CIO atau badan lain mengikut kesesuaian.

Mengambil tindakan terhadap individu yang terlibat setelah berunding dengan kumpulan tindakan, pengarah PPKT, CIO, contohnya menggantung akaun pengguna bagi satu tempoh tertentu, menghalang capaian kepada servis atau denda dalam bentuk kompaun.

5.3.3 Respon kepada Insiden Keselamatan yang Berpotensi

a) Pentadbir TMK dan Pentadbir Keselamatan TMK hendaklah memerhati perlakuan pengguna yang luar biasa dan, jika perlu, membuat penyiasatan.
b) Pentadbir Keselamatan TMK hendaklah mendapatkan lebih banyak bukti sebelum mengambil sebarang tindakan terhadap pengguna tersebut. Pentadbir Keselamatan 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 Keselamatan TMK hendaklah merujuk **Perkara 5.3.2** untuk tindakan selanjutnya.
d) Jika kejadian itu merupakan insiden keselamatan berpotensi, maka Pentadbir Keselamatan 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, penyebaran dan penglibatan dalam program kesedaran keselamatan TMK bagi meningkatkan kemahiran dan pengetahuan tentang keselamatan TMK.

6.3 Garis Panduan

6.3.1 Merancang Program Kesedaran Keselamatan

Program kesedaran hendaklah mengambil kira latar belakang pendidikan, bidang kerja dan pelepasan keselamatan 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 (Rujuk **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 pada Lampiran E: jadual Komponen Program Keselamatan TMK.

7 Pengendalian Insiden Keselamatan TMK *(ICT Security Incident Handling)*

7.1 Pengenalan

Ancaman keselamatan siber yang semakin banyak mengganggu sistem TMK menyebabkan proses menangani sesuatu insiden itu menjadi amat penting untuk mengurangkan kehilangan dan kerosakan. Pentadbir Keselamatan TMK mestilah mengambil tindakan baik pulih bagi menyelesaikan masalah.

7.2 Tujuan

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

a) Menangani insiden atau pelanggaran keselamatan.
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 TMK.
b) Prosedur hendaklah meliputi tindakan-tindakan mengikut keperluan 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.

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.

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 Permakluman Perlaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team (GCERT)* Oleh Agensi Keselamatan Siber Negara (*NACSA*) (28 Januari 2019)**,** setiap agensi kerajaan dikehendaki melaporkan sebarang insiden keselamatan kepada kepada Agensi Keselamatan Siber Negara (*NACSA*). Laporan insiden keselamatan penting bagi

NACSA 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. Semak duga (*Probing*)
ii. Serangan kod jahat (*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 Pelayan (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 tanda-tanda 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 Keselamatan TMK sebaik sahaja insiden itu dikenal pasti dengan mengikuti prosedur pelaporan insiden keselamatan siber yang ada.

7.4.2 Pengumpulan Bukti

Pentadbir Keselamatan TMK hendaklah merekod semua insiden keselamatan yang dikesan mengikut keperluan borang pelaporan insiden tersebut.

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 perkhidmatan TMK 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;
e) perubahan produk atau perkhidmatan daripada penjual atau pembekal; dan
f) Perubahan teknologi.

8.3.2 Jenis-jenis Perubahan

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

a) Perkakasan.
b) Perisian.
c) Proses kerja.
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 mengikut prosedur perkhidmatan masing-masing.
d) Mendokumentasikan semua perubahan dan hasil yang dijangkakan.
e) Melaksanakan pemantauan kepada perubahan yang dilakukan.
f) Melaksanakan prosedur sandaran untuk mendapatkan imej sistem sebelum mewujudkan persekitaran baru.

8.3.4 Maklumat yang Diperoleh

a) Maklumat berikut hendaklah dimasukkan ke dalam Borang Permohonan Perubahan (rujuk 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 sandaran.
    xiii. Semakan semula data dan hasil.

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

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

9 Perlindungan peranti

9.1 Pengenalan

Kod hasad (*malicious code)* seperti virus, perisian intip (*spyware), spam, ransomware* dan perisian cecacing (*worm)* boleh menjangkiti sistem TMK melalui pelbagai kaedah, termasuk emel, rangkaian kerja, Internet dan capaian fail yang dijangkiti virus dari media storan mudah alih. Kod hasad boleh tersebar dengan cepat ke komputer lain dalam rangkaian. Kod hasad boleh menyerang sistem pengoperasian (OS), program aplikasi dan fail-fail yang terkandung di dalam komputer tersebut.

Peranti yang disambungkan ke rangkaian mestilah mempunyai perisian anti kod hasad (*anti malware*) yang sentiasa dikemaskini. Perisian anti kod hasad mestilah dikemaskini dan dipasang dengan fail tampalan kritikal.

Pentadbir TMK yang bertanggung jawab mestilah mengguna pakai sistem perisian anti kod hasad untuk melawan kod hasad pada laluan emel (e*mail gateway*), pelayan, komputer, pelayan dan peranti komputeran yang lain.

9.2 Tujuan

Topik ini bertujuan membantu Pentadbir Keselamatan TMK menghalang kod hasad daripada menyerang/menjangkiti peranti perkomputeran dalam rangkaian dan meminimumkan penyebaran jangkitan.

9.3 Garis Panduan

9.3.1 Pemasangan Perisian Anti-Kod Hasad

a) Semua peranti yang berupaya dipasang perisian anti kod hasad hendaklah dipasang dengan perisian anti kod hasad. Perisian anti kod hasad hendaklah dipasang walaupun peranti itu tidak boleh digunakan untuk mengakses sistem rangkaian kerana kod hasad boleh berada dalam fail tanpa dikesan.

b) Perisian anti kod hasad pada komputer pengguna hendaklah dikonfigurasikan untuk:

i. memuat turun fail definisi kod hasad terkini dari pelayan perisian kod hasad setiap hari;
ii. beroperasi setiap masa secara automatik;
iii. mengaktifkan imbasan ingatan (RAM), *master records* , *boot records atau variasinya*, serta fail sistem semasa memulakan peranti; dan
iv. mengimbas semua fail – kod hasad boleh wujud dalam semua jenis fail dan tidak memadai dengan hanya mengimbas fail program boleh laksana *(executable programmes).*

9.3.2 Konfigurasi Lain

a) Menyekat perlaksanaan fail-fail skrip yang menggunakan teknologi *Script Host* dari sumber yang tidak diketahui.
b) Mengaktifkan Perlindungan Kod Makro.
c) Jangan benarkan lampiran dibuka secara automatik dalam program emel.
d) Tingkatkan ciri-ciri keselamatan yang terdapat dalam perisian digunakan.

9.3.3 Kawalan Integriti Data

a) Pemasangan perisian terkawal seperti perisian rakan ke rakan atau perisian penembusan perlu mendapat kebenaran dari PPKT.
b) Elakkan pemasangan perisian percuma (*freeware*), perisian kongsi (*shareware*) *dari sumber yang tidak diketahui atau diragui* atau perisian yang tidak dibenarkan *(unauthorised software).*
c) Imbas semua program perisian atau fail tampalan sebelum dipasang.
d) Imbas semua media storan mudah alih sebelum diguna.
e) Jika pengguna menghadapi ketidakpastian dan keraguan kepada aplikasi yang ingin dipasang, sila lakukan semakan dengan staf teknikal atau unit yang bertanggunjawab kepada keselamatan TMK.

9.3.4 Kesedaran Keselamatan

a) Memberi kesedaran kepada semua pengguna tentang bahaya kepilan emel, kod hasad, penipuan dan ancaman-ancaman siber yang lain

b) Mendidik pengguna tentang perisian anti kod hasad yang digunakan dan bagaimana ia berfungsi. Hal ini membantu menghapuskan kekeliruan agar pengguna tidak akan melumpuhkan perisian anti kod hasad pada komputer mereka.

9.3.5 Menangani Masalah Kod Hasad

a) Menentukan jenis dan sumber jangkitan.

b) Melaksana tindakan yang perlu untuk meminimumkan jangkitan kod hasad.

9.4 Prosedur

9.4.1 Respon Terhadap Masalah *Malicious Code*

a) Pentadbir Keselamatan TMK perlu mengemaskini fail definisi anti kod hasad pada setiap masa supaya dapat mengenal pasti kod hasad yang memasuki sistem.

b) Semua peranti dalam rangkaian hendaklah diimbas secara manual atau automatik untuk mengenal pasti peranti yang dijangkiti bagi mengesan sumber jangkitan.

c) Semua peranti yang dijangkiti perlu diasingkan untuk mengelakkan jangkitan daripada merebak dengan memutuskan sambungan secara fizikal daripada rangkaian. Sekiranya jangkitan menular, Pentadbir Keselamatan TMK hendaklah menimbang sama ada untuk memutuskan sebahagian atau keseluruhan rangkaian kerana kod hasad berupaya menjejaskan rangkaian lain di dalam atau di luar universiti.

d) Perisian anti kod hasad perlu dilaksanakan pada semua peranti yang dijangkiti bagi memulihkannya dari jangkitan. Semua peranti mestilah dipulihkan kepada tahap asal atau memasang semula sistem pengoperasian (OS) sekiranya perisian anti kod hasad tidak dapat memulihkan jangkitan.

e) Peranti atau rangkaian tidak boleh dihubungkan ke dalam talian sehingga semua kesan kod hasad dihapuskan.

f) Sekiranya Pentadbir Keselamatan TMK tidak dapat mengawal jangkitan kod hasad, maka Pentadbir Keselamatan TMK hendaklah melaporkan insiden ini kepada NACSA.

g) Jangkitan kod hasad 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 tidak boleh diabaikan atau dikesampingkan kerana tidak ada pengganti bagi kawalan keselamatan fizikal yang baik.

10.2 Tujuan

Topik ini bertujuan membantu Pentadbir Keselamatan TMK atau pentadbir TMK menghalang capaian tanpa kebenaran, kerosakan dan gangguan kepada infrastruktur fizikal TMK seperti pelayan 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 yang menjalankan penyelidikan dan bilik pelayan hanya dihadkan kepada individu yang dibenarkan.

10.3.2 Perlindungan Kemudahan dan Keselamatan Bilik Pelayan

a) Pintu dan tingkap hendaklah sentiasa dikunci. Perlindungan keselamatan tambahan hendaklah diambil kira bagi tingkap, khususnya di tingkat bawah.
b) Kelengkapan kawalan hendaklah dipasang untuk meminimumkan risiko ancaman seperti kebakaran, seperti sistem penghadang kebakaran, pengesan asap, penangkap kilat atau alat pemadam api.
c) Kawalan hendaklah dijalankan untuk mengurangkan risiko ancaman yang mungkin berlaku seperti suhu melampau, seperti memasang pendingin hawa dan sistem

pengudaraan. Pendingin hawa di dalam bilik pelayan hendaklah dipasang pada setiap masa.

d) Bahan merbahaya dan mudah terbakar (seperti bekalan secara pukal alat tulis dan kotak kosong) tidak boleh disimpan di dalam bilik pelayan.

e) Pentadbir Keselamatan TMK hendaklah memeriksa keselamatan infrastruktur fizikal TMK sekurang-kurangnya satu (1) kali setahun.

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

10.3.3 Keselamatan Peralatan

a) Semua kelengkapan mestilah dikenalpasti dan direkod.

b) Bekalan kuasa hendaklah stabil dan bebas daripada gangguan.

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

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

e) Semua anak kunci 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 Jabatan Keselamatan USM.

f) Peralatan seperti kabel, pelayan 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 yang dipasang di atas lantai perlu dilindungi.

i) Peralatan hendaklah diletakkan di tempat yang sesuai. Sebagai contoh, pelayan 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) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

l) Pegawai yang menerima peralatan mudah alih hendaklah mengambil langkah-langkah yang perlu untuk memastikan kawalan dan keselamatan peralatan tersebut.

m) Pemilikan aset TMK perlu dikenalpasti dan dikendalikan oleh pengguna yang dibenarkan.

n) Pengguna dan pentadbir TMK hendaklah menentukan tarikh dan masa sistem komputer atau pelayan adalah tepat;

10.3.4 Pengendalian Pelawat

a) Kehadiran pelawat di bilik pelayan hendaklah direkodkan di dalam buku log. Rekod hendaklah mengandungi nama, organisasi, tarikh, masa masuk, masa keluar dan tujuan memasuki tempat tersebut.

b) Kehadiran pelawat di bilik pelayan 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 pelayan hendaklah diawasi atas sebab-sebab keselamatan bagi mengelak berlakunya perkara yang tidak diingini.

10.3.5 Pelupusan Data

a) Storan pada komputer dan pelayan yang hendak dikitar semula hendaklah dipadam dengan menggunakan perisian khas pemusnah data.

b) Perisian khas pemusnah data perlu disahkan oleh Pentadbir Keselamatan TMK keberkesanannya bagi memastikan data pada storan benar-benar terhapus.

c) Bagi storan yang tidak boleh dikitar semula atau ingin dilupuskan sepenuhnya perlu dimusnahkan secara fizikal dengan cara yang tidak memungkinkan data diselamatkan dari storan tersebut.

11 Pertukaran Maklumat

11.1 Pengenalan

Pertukaran maklumat memainkan peranan penting dalam hubungan antara pengguna TMK samada ianya untuk urusan rasmi atau pun sebaliknya. Pelbagai kaedah pertukaran maklumat boleh dilaksanakan sama ada secara fizikal (seperti CD, DVD, storan mudah alih) atau pun secara maya (seperti emel, FTP, muat turun/muat naik, menggunakan media sosial).

11.2 Tujuan

Topik ini bertujuan membantu Pentadbir Keselamatan TMK menasihati para pengguna TMK di dalam USM untuk sentiasa berwaspada dan memastikan keselamatan pertukaran maklumat dan perisian antara USM dan agensi luar terjamin.

11.3 Garis Panduan

11.3.1 Pengurusan Pertukaran Maklumat

a) Sebarang pertukaran maklumat perlu mendapat kebenaran daripada pemilik data terlebih dahulu.
b) Perjanjian kerahsiaan perlu diwujudkan untuk pertukaran maklumat dan perisian di antara USM dengan agensi luar.
c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan; dan
d) Maklumat yang dikelaskan sebagai terkawal yang dikongsi melalui perantaraan elektronik perlu dilindungi sebaik-baiknya termasuk penggunaan penyulitan atau perkongsian dengan kata laluan.
e) Maklumat-maklumat yang diletakkan di laman sesawang adalah tertakluk kepada batasan kerahsiaan maklumat. Sebelum sesuatu maklumat bersifat terhad yang hendak diletakkan di laman sesawang, ia mestilah diperiksa dan

diluluskan untuk siaran, mengikut prosedur seperti mana sebelum sesuatu memo, laporan atau maklumat-maklumat rasmi lain disiarkan.

11.3.2 Pengurusan Mel Elektronik (Emel)

Penggunaan emel di USM hendaklah dipantau secara berterusan oleh Pentadbir Emel untuk memenuhi keperluan etika penggunaan emel mengikut undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi dalam pengendalian emel adalah seperti berikut:

a) Semua mesej dari luar yang memasuki rangkaian USM hendaklah diperiksa untuk menyekat virus, spam, phishing dan ancaman keselamatan yang lain;
b) Akaun atau alamat emel yang diperuntukkan oleh USM sahaja boleh digunakan. Penggunaan akaun milik orang lain adalah dilarang;
c) Pengguna perlu memastikan alamat emel penerima adalah betul;
d) Penggunaan fail kepilan tidak melebihi had kekangan semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz atau perkongsian melalui storan Internet yang disediakan adalah disarankan. Fail kepilan yang hendak dihantar tiada dalam jenis fail yang dilarang.
e) Fail-fail kepilan yang melebihi had kekangan atau ditujukan kepada ramai penerima perlu dihoskan pada storan Internet yang disediakan. Hanya pautan kepada fail tersebut sahaja dihantar kepada penerima.
f) Pengguna hendaklah mengelak dari membuka emel daripada penghantar yang tidak diketahui atau diragui.
g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel.
h) Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan dengan baik.

i) Emel yang tidak penting dan tidak mempunyai nilai arkib dan tidak diperlukan dinasihat untuk dihapuskan.

j) Pengguna hendaklah memastikan emel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak digunakan untuk tujuan rasmi.

k) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan akaun emel masing-masing.

l) Dilarang menghebahkan sebarang hebahan yang berunsur negatif (seperti politik, perjudian, jenayah dan radikal) dan perniagaan yang mendatangkan keuntungan peribadi.

m) Pemohon bertanggungjawab sepenuhnya untuk memastikan kesahihan dan ketepatan maklumat yang dihantar melalui emel.

n) Penggunaan yang keterlaluan untuk tujuan peribadi adalah tidak digalakkan.

11.3.3 Storan Internet

Perkara-perkara yang perlu dipatuhi dalam pengendalian storan Internet yang disediakan oleh USM adalah seperti berikut:

a) Penggunaan storan Internet diberi keutamaan untuk kegunaan rasmi.

b) Fail-fail sulit pada storan Internet hanya dibenarkan dikongsi dengan individu yang dibenarkan dan dikawal capaiannya.

c) Pengguna tidak dibenarkan untuk berkongsi akaun storan Internet kepada individu lain untuk digunakan.

d) Akses kepada storan Internet hendaklah dikawal mengikut tahap capaian pengguna.

12 Pembangunan dan Pengurusan Aplikasi

12.1 Pengenalan

Pembangunan dan pengurusan aplikasi merupakan proses yang diwujudkan untuk mengurus dan mengawal selia keselamatan dalam pembangunan aplikasi secara dalaman atau pembangunan aplikasi yang disumber luarkan. Pembangun aplikasi, termasuk pihak ketiga perlu mengadaptasi standard pengurusan pembangunan, pengujian, pemasangan dan penyelenggaraan yang selamat.

12.2 Tujuan

Topik ini bertujuan menyediakan garis panduan untuk meningkatkan tahap keselamatan dalam aplikasi dan membantu menjaga sumber-sumber teknologi maklumat universiti.

Pematuhan kepada keperluan ini perlu diintegrasikan ke dalam pelan keselamatan sistem yang komprehensif bagi membolehkan kawalan menyeluruh kepada aplikasi yang dibangunkan dan diguna pakai oleh universiti.

12.3 Garis Panduan

12.3.1 Pembangunan Aplikasi

a) Memastikan aplikasi membuat semakan pengesahan kepada data yang dimasukkan oleh pengguna dengan menyediakan proses pengesahan maklumat (*input validation*) sebelum data disimpan ke storan atau pangkalan data.

b) Memastikan aplikasi melaksanakan pengendalian ralat yang betul supaya kesilapan tidak akan memberikan maklumat sistem secara terperinci, merosakkan mekanisma keselamatan atau merosakkan sistem.

c) Memastikan aplikasi yang memerlukan pengesahan pengguna menggunakan pengesahan secara berpusat.

d) Memastikan aplikasi menggunakan storan penyimpanan selamat untuk data-data universiti, terutama data berimpak yang tinggi, sensitif atau memerlukan pematuhan standard.

e) Memastikan aplikasi usang dikeluarkan dari sebarang persekitaran yang memungkinkan perlaksanaannya.

f) Aplikasi yang dibangunkan secara sumber luar perlu mendapat persetujuan secara bertulis daripada pihak pengurusan universiti dan mematuhi garis panduan berkaitan keselamatan maklumat bagi memastikan keselamatan aplikasi dan data univerisiti.

g) Mengasingkan pelayan dan pangkalan data yang digunakan dalam pembangunan dan operasi.

h) Pengujian kepada aplikasi perlu dilaksanakan sebelum aplikasi digunakan dalam pelayan operasi.

i) Pengujian keselamatan kepada aplikasi perlu dilakukan secara berkala pada pelayan pembangunan atau pelayan operasi mengikut kesesuian dan keperluan.

j) Repositori kod sumber dan media-media yang digunakan oleh aplikasi perlu diwujudkan bagi tujuan penyimpanan, pengawalan versi dan dokumen.

k) Capaian kepada kod sumber dan media perlu dikawal dan sebarang perubahan perlu direkod.

l) Kod sumber aplikasi perlu dinilai (*review*) sama ada secara manual atau automatik, sebarang pembaikan kritikal perlu dilakukan sebelum ia digunakan pada pelayan operasi.

m) Semua laman-laman sesawang yang boleh diakses oleh orang awam mestilah diuji dengan penuh teliti bagi memastikan kesemua sambungan (links) berfungsi mengikut sebagaimana yang dikehendaki. Laman-laman sesawang yang masih di dalam pembinaan tidak dibenarkan untuk kegunaan awam.

12.3.2 Pengurusan Aplikasi

a) Maklumat yang dikelaskan sebagai rahsia dan terhad (seperti nombor kad pengenalan atau passport, maklumat kesihatan yang dilindungi, maklumat berkaitan kewangan, pemarkahan dan lain-lain maklumat) tidak boleh didedahkan kecuali kepada individu- yang dibenarkan.

b) Mengemaskini inventori penuh bagi semua aplikasi yang merangkumi penerangan sistem, termasuk Pentadbir TMK yang bertanggung jawab.

c) Pentadbir TMK atau pihak ketiga yang mentadbir aplikasi yang berkaitan dengan data Universiti atau terlibat dengan pembangunan atau menganalisis aplikasi perlu disahkan dan dipersetujui oleh pihak pengurusan PPKT atau Universiti.

13 Keselamatan Rangkaian dan Telekomunikasi

13.1 Pengenalan

Komunikasi bermaksud menghantar dan menerima maklumat menerusi wayar atau tanpa wayar secara elektronik. Contoh-contoh teknologi tersebut ialah rangkaian (data, audio dan video) termasuk sistem telefoni, telesidang video dan Internet.

13.2 Tujuan

Topik ini bertujuan menyediakan garis panduan untuk meningkatkan tahap keselamatan dalam perkhidmatan berkaitan dengan rangkaian dan telekomunikasi dan pemantuan yang perlu dilakukan oleh pengguna, Pentadbir TMK dan Pentadbir Keselamatan TMK.

13.3 Garis Panduan

13.3.1 Infrastuktur Rangkaian dan Telekomunikasi

a) Sebarang perkakasan yang hendak dipasang mestilah telah menjalani *Factory Acceptance Check* (FAC), sebelum pemasangan dijalankan;

b) Perkakasan rangkaian dan telekomunikasi hendaklah ditempatkan di lokasi yang secara fizikalnya kebal dan bebas daripada risiko yang tidak boleh diterima seperti banjir, getaran, debu dan lain-lain;

c) Bekalan kuasa kepada semua perkakasan hendaklah bebas dari gangguan dan perubahan secara tidak nalar;

d) Semua perkakasan rangkaian dan telekomunikasi hendaklah ditempatkan secara fizikalnya selamat, di mana hanya akses terhad sahaja dibenarkan;

e) Akses kepada rangkaian dan telekomunikasi mestilah dikawal rapi dengan menggunakan suatu sistem kawalan pengesahan pengguna/rangkaian (*user/network authentication control system*);

f) Akses kepada perkakasan rangkaian dan telekomunikasi hendaklah dikawal oleh kawalan-kawalan akses logikal, bersesuaian dengan peranan Pentadbir TMK atau individu yang dibenarkan.;

g) Semua pengkabelan rangkaian dan telekomunikasi hendaklah dihoskan dengan selamat dari aspek fizikal dari kerosakan atau pencerobohan;

h) Sebarang pemasangan peralatan rangkaian dan telekomunikasi seperti pemasangan *access point* (AP) mestilah mendapat kebenaran daripada Pengarah PPKT;

i) Hanya perkhidmatan yang perlu sahaja dibenarkan di dalam rangkaian dan capaian kepada perkhidmatan melalui konfigurasi rangkaian kerja yang selamat, termasuk tapisan firewall, Sistem Pengesanan/Pencegahan Pencerobohan dan sistem log masuk yang sesuai;

j) aktiviti kritikal di dalam rangkaian hendaklah disimpan di dalam fail log;

k) *Sniffer* atau *network analyser* adalah sama sekali tidak dibenarkan kecuali dengan kebenaran pentadbir TMK setelah mendapat kebenaran dari Pengarah PPKT;

l) Penapis paket(IPS/IDS atau *firewall)* hendaklah dipasang di antara rangkaian-rangkaian dalaman;

m) Kebenaran khas hendaklah dipohon daripada Pengarah PPKT untuk tujuan penyambungan ke mana-mana rangkaian dan telekomunikasi yang bukan di bawah kawalan Universiti;

n) Pemasangan protokol rangkaian hendaklah dikurangkan dan hanyalah mengikut keperluan.

o) Semua trafik yang masuk dan keluar daripada sistem rangkaian Universiti mestilah melalui *firewall*;

p) *Firewall* hendaklah dikonfigurasikan untuk membenarkan hanya trafik tertentu sahaja boleh melintasinya;

q) Sebarang transmisi dokumen rahsia seperti kata laluan, mestilah disulitkan;

r) Alat-alat pemantau rangkaian seperti Sistem Pengesanan/Pencegahan Pencerobohan mestilah dipasang untuk mengesan/mencegah cubaan-pencerobohan atau menyeleweng dari perilaku kebiasaan.

s) Pengguna dilarang dengan sengaja menghantar atau menyimpan apa-apa bahan atau mesej-mesej dengan jelas sensitif kepada perkauman, kebudayaan atau seksual;

t) Pengguna dilarang menyalin bahan-bahan yang dipaten atau dengan Hak Milik Terperlihara, termasuk teks, kod program atau data, tanpa kebenaran daripada pemilik bahan-bahan tersebut.

u) Pengguna dilarang melakukan sebarang aktiviti yang boleh mengganggu perjalanan perkakasan atau sistem.

v) Pengguna dilarang dari cuba memasuki atau menggunakan mana-mana sistem komputer atau rangkaian kecuali telah diberi kebenaran oleh pemilik sistem tersebut, atau sistem tersebut telah diisytiharkan sebagai sistem kegunaan awam.

w) Sebarang permohonan akses kawalan jauh (remote access) ke rangkaian kerja Universiti dari luar perlu membuat permohonan rasmi dan dimajukan kepada pengarah PPKT untuk kelulusan.

x) Pelayan yang disambung ke rangkaian perlu didaftarkan dan mempunyai maklumat nama komputer, servis/port dan maklumat Pegawai TMK atau individu yang bertanggungjawab.

14 Penggunaan Peranti Peribadi (*Bring Your Own Device* , BYOD)

14.1 Pengenalan

Penggunaan BYOD merupakan persetujuan yang membolehkan pengguna menggunakan peranti peribadi mereka seperti telefon bimbit, *tablet*, atau komputer bagi membolehkan mereka melaksanakan tugasan pejabat dan peribadi. Penggunaan peralatan sendiri boleh memberi penjimatan kepada universiti tetapi mendedahkan maklumat jabatan kepada risiko keselamatan.

14.2 Tujuan

Topik ini bertujuan untuk memberikan panduan dan gesaan pematuhan kepada pengguna dalam menggunakan peranti peribadi.

14.3 Garis Panduan

a) Peranti yang digunakan perlu dilindungi dengan perisian anti kod hasad dan *firewall* peribadi.

b) Peranti yang digunakan perlu dikemaskini tampalan dengan menggunakan versi terkini dan stabil.

c) Peranti yang digunakan perlu dilindungi dengan penggunaan kata laluan atau mekanisma sekuriti yang lain.

d) Peranti yang mempunyai isu keselamatan yang dikompromi atau dipasang dengan perisian yang mempunyai risiko keselamatan seperti perisian cetak rompak atau perisian yang tidak diketahui risiko keselamatannya, tidak dibenarkan untuk digunakan sebagai peranti BYOD.

e) Peranti yang digunakan hendaklah dikonfigurasikan dengan penyulitan kepada ruang storan seperti penggunaan *Bitlocker*, TPM atau direktori yang disulit.

f) Peranti perlu mempunyai fungsi pemadaman data secara jauh (*remove wipe*) yang diaktifkan.

g) Keserasian peranti dan capaian kepada sumber komputeran universiti adalah di bawah tanggungjawab pengguna.

h) Pihak universiti tidak bertanggungjawab atas sebarang insiden yang melibatkan kerosakan kepada peranti peribadi pengguna.

i) Maklumat berkaitan urusan kerja perlu dihapuskan dari peranti apabila pengguna tidak lagi berkhidmat dengan universiti.

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 pelayan, makmal komputer dikawal dan dihadkan kepada individu yang dibenarkan?				
	2. Adakah bilik pelayan 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 pelayan?				
	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 TMK (pelayan/komputer) dan kabel dilabel dengan betul?				

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
	10. Adakah kabel dipasang dengan teratur?				
	11. Adakah kelengkapan TMK diselenggara secara berkala?				
2. Sandaran (Backup)	1. Adakah media sandaran 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 sandaran 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?				
	1. Adakah proses pengurusan perubahan dipatuhi apabila Sistem sebarang perubahan dibuat kepada pelayan?				

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
5. Penyelenggaraan Sistem	2. Adakah sistem sentiasa dipantau dan dikemas kini apabila terdapat fail kemas kini dan fail tampalan 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 tujuh (7) kali berturut-turut?				
8. Pengurusan Kata Laluan	1. Adakah kata laluan pengguna digalakkan ditukar setiap 180 hari?				
	2. Adakah kata laluan mempunyai sekurang-kurangnya lapan (8) aksara yang terdiri daripada angka abjad (*alphanumeric*) dan simbol?				
	3. Adakah pengguna dibenarkan mengguna semula empat (4) kata laluan yang terdahulu?				
	4. Adakah kata laluan dipaparkan sebagai teks jelas pada skrin apabila dimasukkan?				
	5. Adakah kata laluan pelayan disimpan dalam bentuk teks jelas?				

Tajuk Dokumen	:	GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI UNIVERSITI SAINS MALAYSIA
No. Terbitan	:	3.1
Tarikh Kuatkuasa	:	18 APRIL 2023

Bidang Kawalan	Keadaan	Ya	Tidak	Tiada	Ulasan
	6. Adakah semua komputer meja dan peranti mudah alih (contohnya komputer riba) dipasang dengan perisian anti kod hasad?				
9. Anti-Malicious Code	1. Adakah fail definisi perisian anti kod hasad dikemas kini secara berkala untuk pelayan, 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 : .....

Lampiran B – Contoh Notis bagi Penyalahgunaan Sumber TMK

NOTIS PEMBERITAHUAN

Kepada : Ketua Pegawai Maklumat Tarikh <Tarikh>

Daripada : <Pentadbir Keselamatan 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 Keselamatan 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 Keselamatan 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 – 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?

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 :

Tarikh :

Perubahan yang dicadangkan di atas:

❑ Berjaya dilaksanakan pada : _____

❑ Tidak berjaya kerana: _____

Disemak oleh,

.....

Nama :

Tarikh :

Lampiran E – Jadual Komponen Program Keselamatan TMK

	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

Lampiran F – Maklumat Pihak Bertanggungjawab Bagi Pengendalian Insiden

a) Meja Bantuan

Servisdesk@PPKT

Pusat Pengetahuan, Komunikasi & Teknologi

Universiti Sains Malaysia

No. Tel. : 04-653 4400

No. Faks : 04-656 1012

E-mel : servisdesk@usm.my

Web: https://sd.usm.my

b) Pegawai Keselamatan Maklumat

e-mel: infosec@usm.my

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.
Kod Hasad (*Malicious Code*)	Kod yang dimuatkan ke dalam komputer tanpa pengetahuan dan kebenaran pemilik, khusus untuk merosakkan atau melumpuhkan sistem seperti virus, cecacing atau *trojan.*
Rakan ke rakan (*Peer-to-peer*)	Sejenis rangkaian yang setiap stesen kerja mempunyai keupayaan dan tanggungjawab yang sama.
Semak duga (*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 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 Pelayan *(Pelayan Room)*	Bilik yang menempatkan komputer/pelayan yang membolehkan perkongsian sumber seperti pencetak dan fail.
Perisian Kongsi *(Shareware)*	Perisian percuma yang boleh dicuba untuk tempoh tertentu sebelum dibeli sepenuhnya.
Perisian Intip (*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.

ServisDesk

Bertindak sebagai meja bantuan TMK bagi menangani sebarang aduan/masalah yang dilaporkan oleh pengguna TMK. Meja bantuan boleh dihubungi seperti berikut:

i. Kampus Induk, Pulau Pinang (Tel: 04 653 4400, e-mel: servisdesk@usm.my, laman sesawang: servisdesk.usm.my, kaunter: Aras 2, Kompleks Eureka)

ii. Kampus Kejuruteraan: (Tel: 04 599 5333, e-mel: servisdesk.eng@usm.my)

iii. Kampus Kesihatan : (Tel: 09 767 1111, e-mel: techsupport@usm.my)

iv. Institut Perubatan dan Pergigian Termaju (Tel: 04 562 2111, e-mel: servisdesk@usm.my)

RUJUKAN

1. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000
2. Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) bertarikh 15 Jan 2002
3. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 Nov 2005
4. Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 17 Nov 2009
5. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010
6. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010
7. Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010
8. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam
9. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
10. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
11. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
12. Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022
13. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022