1. TUJUAN

1.1 Panduan ini disediakan sebagai rujukan kepada warga Universiti Malaysia Kelantan (UMK) untuk mematuhi dan melaksanakan langkah-langkah keselamatan perlindungan mengikut dasar yang ditetapkan oleh kerajaan bagi memastikan keselamatan dan kerahsiaan rahsia rasmi khususnya berkaitan pengurusan mesyuarat diberikan perlindungan.

2. LATAR BELAKANG

2.1 Universiti Malaysia Kelantan (UMK) melalui Pekeliling Pentadbiran Bilangan 21 Tahun 2020 telah mengeluarkan Panduan Pengurusan Mesyuarat UMK. Panduan tersebut menerangkan tatacara pengurusan mesyuarat secara manual dan digital ke arah pengendalian mesyuarat yang lebih sistematik, seragam dan efektif.

2.2 Penularan pandemik Covid-19 telah memberi impak besar kepada dunia termasuklah dalam pengurusan dan pengendalian mesyuarat. Bermula tahun 2020, pelaksanaan mesyuarat dalam talian telah dilaksanakan secara meluas sebagai norma baharu dalam kehidupan serta cara kerja.

2.3 Walaupun pelaksanaan mesyuarat dilaksanakan mengikut norma baharu, aspek keselamatan dokumen dan kerahsiaan mesyuarat perlu turut diberi perhatian. Sehubungan itu, selaras dengan keperluan tersebut, UMK menyediakan Panduan Pengurusan Keselamatan dan Kerahsiaan Mesyuarat sebagai melengkapi panduan sedia ada.

2.4 Panduan Pengurusan Keselamatan dan Kerahsiaan Mesyuarat ini perlu dibaca bersama dokumen berikut:

a. Panduan Pengurusan Mesyuarat Universiti Malaysia Kelantan seperti di **Lampiran A.**

b. Surat Pekeliling Am Bilangan 1 Tahun 2021 - Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi Dan Segala Peralatan Elektronik Yang Mampu Merakam Maklumat Dalam Mesyuarat Penting Kerajaan seperti di **Lampiran B.**

c. Dasar Keselamatan ICT Universiti Malaysia Kelantan seperti di **Lampiran C.**

3. TANGGUNGJAWAB PENGURUSAN KESELAMATAN DAN KERAHSIAAN MESYUARAT

3.1 Tanggungjawab Setiausaha/ Urus Setia Mesyuarat

a. Memastikan pengurusan dokumen mesyuarat hanya dikendalikan oleh staf yang lulus tapisan keselamatan dan bertanggungjawab terhadap sesuatu mesyuarat tersebut sahaja.

b. Menyediakan borang *integrity pact* bagi setiap mesyuarat. Templat *integrity pact* adalah seperti di **Lampiran D**. Bagi mesyuarat secara dalam talian, setiausaha/ urus setia hendaklah menyediakan borang *integrity pact* dalam bentuk *google form* atau kaedah lain yang sesuai. Borang *integrity pact* tersebut hendaklah dicetak dan disimpan di dalam fail mesyuarat untuk rekod.

c. Memastikan dokumen mesyuarat dihantar/ dikemukakan dengan selamat kepada ahli mesyuarat. Setiausaha/ Urus Setia boleh menggunakan sistem emeeting, platform *google drive* atau kaedah-kaedah lain yang sesuai dan selamat. Sekiranya platform secara dalam talian selain sistem emeeting digunakan, dokumen mesyuarat hendaklah diletakkan *password* (kaedah *encryption*).

d. Memastikan setiap ahli mesyuarat menandatangani *integrity pact* sebelum sesuatu mesyuarat dimulakan.

e. Memaparkan taklimat integriti sebelum mesyuarat bermula.

f. Memastikan rakaman rekod mesyuarat di dalam perakam suara (atau rekod melalui aplikasi mesyuarat dalam talian) dipadamkan daripada peranti tersebut setelah disimpan oleh setiausaha/ urus setia sejurus selepas mesyuarat selesai. Rakaman rekod mesyuarat hendaklah disimpan dengan selamat oleh setiausaha/ urus setia dan jangan sesekali disimpan di dalam komputer riba umum/ guna sama. Rakaman rekod mesyuarat hendaklah dilupuskan selepas enam (6) bulan dari tarikh mesyuarat.

g. Tidak mengedarkan rakaman rekod mesyuarat kepada ahli mesyuarat.

h. Memastikan hanya setiausaha/ urus setia yang boleh merekodkan mesyuarat dalam talian. Ahli mesyuarat lain tidak dibenarkan membuat perekodan.

i. Memastikan dokumen mesyuarat tidak ditinggalkan di bilik mesyuarat.

j. Memastikan dokumen mesyuarat disimpan di tempat yang selamat dan tidak terdedah kepada pihak yang tidak sepatutnya.

k. Menjaga kerahsiaan mesyuarat. setiausaha/ urus setia tidak boleh membocorkan keputusan mesyuarat sebelum keputusan secara rasmi dikeluarkan.

l. Tidak membocorkan atau memanipulasi apa-apa maklumat yang dibincangkan dalam mesyuarat kepada pihak yang tidak sepatutnya.

m. Minit Mesyuarat

    a. Minit mesyuarat hendaklah mempunyai nombor rujukan.

b. Minit mesyuarat yang diperingkatkan hendaklah diberi tanda mengikut peringkat yang telah ditetapkan iaitu ‘RAHSIA BESAR’, ‘RAHSIA’, ‘SULIT’ atau ‘TERHAD’ di kiri *header* dan kanan *footer* pada setiap muka surat.

3.2 Tanggungjawab Pengerusi/ Ahli Mesyuarat

a. Memastikan setiap ahli mesyuarat menandatangani/ mengisi *integrity pact* sebelum sesuatu mesyuarat dimulakan atau selewat-lewatnya sebelum ahli meninggalkan mesyuarat.

b. Sentiasa mengingatkan ahli mesyuarat supaya sentiasa menjaga kerahsiaan mesyuarat.

c. Menandatangani/ mengisi *integrity pact* sebelum sesuatu mesyuarat dimulakan.

d. Memastikan peranti kamera yang digunakan bagi mesyuarat secara dalam talian sentiasa dipasang sepanjang mesyuarat berlangsung.

e. Tidak mengambil gambar/ video/ *screen shot* sebarang dokumen/ pembentangan mesyuarat tanpa kebenaran.

f. Menjaga kerahsiaan mesyuarat. Tidak membocorkan keputusan mesyuarat sebelum keputusan secara rasmi dikeluarkan.

g. Tidak membocorkan atau memanipulasi apa-apa maklumat yang dibincangkan dalam mesyuarat kepada pihak yang tidak sepatutnya.

4. LARANGAN PENGGUNAAN TELEFON BIMBIT, PERALATAN KOMUNIKASI DAN SEGALA PERALATAN ELEKTRONIK YANG MAMPU MERAKAM MAKLUMAT DALAM MESYUARAT PENTING

4.1 Naib Canselor atau pengerusi mesyuarat hendaklah menetapkan mana-mana Mesyuarat penting untuk dikuatkuasakan zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat mesyuarat.

4.2 Penetapan tersebut hendaklah mengambil kira risiko sekiranya sesuatu maklumat rasmi atau rahsia rasmi didedahkan melalui telefon bimbit atau peralatan komunikasi lain sebelum keputusan mesyuarat dikeluarkan secara rasmi.

4.3 Kaedah bagi melaksanakan peraturan atau ketetapan ini hendaklah berpandukan kepada Surat Pekeliling Am Bilangan 1 Tahun 2021 - Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi dan Segala Peralatan Elektronik Yang Mampu Merakam Maklumat Dalam Mesyuarat Penting Kerajaan.

5. TINDAKAN TERHADAP STAF YANG MEMBOCORKAN RAHSIA RASMI ATAU MEMANIPULASI MAKLUMAT MESYUARAT

5.1 Staf yang membocorkan atau memanipulasi rahsia rasmi akan dikenakan tindakan tatatertib di bawah Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 [Akta 605] dan boleh dikenakan tindakan undang-undang oleh pihak berkuasa di bawah Akta Rahsia Rasmi 1972 (Akta 88) atau di bawah akta/ peraturan lain yang berkaitan.

6. PEMAKAIAN

6.1 Panduan ini adalah terpakai untuk semua mesyuarat utama Universiti dan juga dipanjangkan kepada mesyuarat lain di peringkat Pusat Tanggungjawab (PTj) yang terlibat dengan perkara rahsia rasmi.

6.2 Panduan ini boleh berubah dari semasa ke semasa tertakluk kepada arahan yang dikeluarkan oleh Kerajaan atau Pengurusan Universiti.

7. RUJUKAN

7.1 Panduan Pengurusan Mesyuarat Universiti Malaysia Kelantan.

7.2 Surat Pekeliling Am Bilangan 1 Tahun 2021 - Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi Dan Segala Peralatan Elektronik Yang Mampu Merakam Maklumat Dalam Mesyuarat Penting Kerajaan.

7.3 Dasar Keselamatan ICT Universiti Malaysia Kelantan.

LAMPIRAN A

PANDUAN PENGURUSAN MESYUARAT UNIVERSITI MALAYSIA KELANTAN

1. TUJUAN

1.1. Panduan ini bertujuan untuk menerangkan kepada staf UMK berkaitan tatacara pengurusan mesyuarat secara manual dan digital ke arah pengendalian mesyuarat yang lebih sistematik, seragam dan efektif.

2. LATAR BELAKANG

2.1. Mesyuarat merupakan satu bentuk komunikasi formal yang dianjurkan di UMK bertujuan untuk membuat sesuatu keputusan atau menyelesaikan sebarang masalah berbangkit.

2.2. Pihak Kerajaan menerusi Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) telah mengeluarkan beberapa panduan mengenai mesyuarat seperti Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 1991 Panduan Pengurusan Mesyuarat dan yang terkini Pekeliling Transformasi Pentadbiran Awam Bilangan 2 Tahun 2018 bertajuk MyMesyuarat : Ekosistem Pengurusan Mesyuarat Era Digital.

2.3. Sejak dari awal penubuhan, UMK telah membangunkan beberapa dokumen berkaitan panduan, peraturan, tatacara pengurusan mesyuarat serta panduan kertas kerja bagi kelulusan Mesyuarat Jawatankuasa Utama Universiti seperti Jawatankuasa Pengurusan Universiti (JPU) dan Lembaga Pengarah Universiti (LPU). UMK menerusi Pusat Komputeran dan Informatik (CCI) juga telah menggunapakai sistem eMeeting dimana satu portal yang mengumpulkan segala rekod bagi mesyuarat utama Universiti.

2.4. Antara dokumen yang telah dikeluarkan adalah seperti berikut;

(i) Tatacara Pengurusan Mesyuarat
(ii) Garis Panduan Penyediaan Kertas Kerja
(iii) Nota Catatan Menghadiri Mesyuarat
(iv) Tatacara Mesyuarat Jawatankuasa Eksekutif (JE)

(v) Polisi Sistem Pengurusan Mesyuarat

(vi) Garis Panduan Penyediaan Kertas Kerja Untuk kelulusan / makluman Mesyuarat Lembaga Pengarah / Jawatankuasa Pengurusan Universiti Malaysia Kelantan

2.5. Dalam menjamin kelestarian pengurusan mesyuarat UMK berkembang dengan transformasi penyampaian perkhidmatan melibatkan mesyuarat-mesyuarat utama UMK, pengemaskinian dalam panduan pengurusan mesyuarat menerusi pemakaian panduan ini adalah perlu kepada semua staf di Universiti Malaysia Kelantan.

3. TAKRIFAN

3.1. Takrifan yang akan diguna pakai dalam garis panduan ini adalah seperti yang berikut:

(i) **Dokumen** merujuk kepada maklumat secara bercetak atau digital dalam bentuk slaid/kertas/cakera padat/video atau medium perantaraan lain yang difikirkan sesuai.

(ii) **Kertas Pembentangan** merujuk kepada Kertas Kerja Kelulusan/Kertas Kerja Makluman bagi mendapatkan keputusan atau memaklumkan kepada ahli mesyuarat.

(iii) **Urus Setia** merujuk kepada urus setia mesyuarat, iaitu sekretariat atau sekumpulan pekerja yang mengendalikan hal-hal pentadbiran dan keurusetiaan mesyuarat.

(iv) **Sistem eMeeting** merujuk kepada modul dalam portal eComm yang menempatkan sistem pengurusan mesyuarat utama UMK

4. KEPERLUAN

4.1. Keberkesanan tadbir urus pelaksanaan sesuatu keputusan mesyuarat sangat berkait rapat dengan kaedah penyampaian keputusan mesyuarat serta kaedah pemantauan tindakan kepada keputusan berkenaan.

4.2. Mesyuarat merupakan satu mekanisme utama yang digunakan untuk:

(i) merancang pelaksanaan sesuatu dasar dan program Universiti;

(ii) memperoleh nasihat daripada pihak yang mempunyai kepakaran dan pengalaman dalam perkara tertentu;

(iii) menyelaras dan memantau usaha-usaha pelaksanaan sesuatu program supaya tindakan yang dilakukan oleh semua yang terlibat dibuat secara bersepadu;

(iv) membuat keputusan secara kolektif melalui perbincangan dan perundingan; dan

(v) menyelesaikan masalah yang timbul dalam melaksanakan sesuatu keputusan.

5. PELAKSANAAN

5.1. Bagi memantapkan pengurusan mesyuarat UMK, maka panduan ini dihasilkan dengan memfokuskan elemen utama seperti yang berikut:

(i) Tanggungjawab Urus Setia Mesyuarat:

A. Peringkat I: Tindakan Sebelum Mesyuarat;
B. Peringkat II: Tindakan Semasa Mesyuarat dan;
C. Peringkat III: Tindakan Selepas Mesyuarat.

(ii) Format Penyediaan Minit Mesyuarat.

5.2. Bagi urusan mesyuarat yang melibatkan dokumen terperingkat, UMK hendaklah mematuhi tata cara pengurusan dokumen terperingkat seperti yang berikut:

(i) Akta Rahsia Rasmi 1972 (Pindaan) 1986; dan

(ii) Arahan Keselamatan.

6. TANGGUNGJAWAB URUS SETIA MESYUARAT

6.1. Kelancaran pengendalian mesyuarat amat bergantung kepada kecekapan urus setia merancang persiapan mesyuarat serta menyediakan pelaporan mesyuarat dalam bentuk minit mesyuarat yang tepat dan berkualiti. Bagi memastikan kelancaran urusan mesyuarat, urus setia perlu memberi perhatian kepada tiga (3) peringkat tanggungjawab urus setia mesyuarat.

6.2. PERINGKAT I: TINDAKAN SEBELUM MESYUARAT

6.2.1. Sebelum mesyuarat dijalankan, urus setia hendaklah membuat persiapan seperti berikut:

(i) Menentukan Agenda, Tarikh, Masa dan Tempat Mesyuarat Bersama Pengerusi Mesyuarat.

1) Urus setia hendaklah memastikan agenda, tarikh, masa dan tempat mesyuarat dipersetujui oleh Pengerusi Mesyuarat.

2) Agenda mesyuarat hendaklah mengandungi perkara-perkara seperti yang berikut:

a) Perutusan Pengerusi Mesyuarat;

b) Pengesahan Minit Mesyuarat / Memorandum Tindakan Pelaksanaan;

c) Perkara-Perkara Berbangkit;

d) Pembentangan Kertas;

e) Hal-Hal Lain; dan

f) Penutup.

3) Urus setia perlu melengkapkan butiran mesyuarat ke dalam Sistem eMeeting seperti tajuk mesyuarat, bilangan mesyuarat, tarikh mesyuarat diadakan, tempat diadakan, tarikh akhir pengesahan kehadiran serta agenda mesyuarat. Urus setia perlulah mengemas kini keahlian eMeeting mengikut terma rujukan yang telah ditetapkan dalam jawatankuasa mesyuarat masing-masing.

(ii) Membuat Tempahan Bilik Mesyuarat

1) Urus setia hendaklah membuat tempahan bilik mesyuarat secara bertulis atau melalui sistem tempahan dalam talian mengikut PTj masing-masing sekiranya ada. Maklumat berhubung tempahan hendaklah dikemukakan kepada pegawai yang bertanggungjawab menerima tempahan. Antara maklumat yang perlu dikemukakan ialah:

a) Nama mesyuarat;

b) Nama dan jawatan Pengerusi Mesyuarat;

c) Nama dan maklumat perhubungan urus setia mesyuarat;

d) Tarikh, masa bermulanya mesyuarat dan masa mesyuarat dijangka tamat;

e) Bilangan ahli mesyuarat;

f) Peralatan yang diperlukan di dalam bilik mesyuarat;

(iii) Menguruskan Kertas-Kertas Pembentangan

1) Kertas pembentangan (sekiranya ada) yang telah dikenal pasti untuk dibentangkan semasa mesyuarat hendaklah dikemukakan bagi pertimbangan dan persetujuan Pengerusi Mesyuarat;

2) Surat panggilan pemakluman pembentangan kertas dihantar kepada ahli mesyuarat atau mana-mana pihak yang diberi tanggungjawab membuat pembentangan sekurang-kurangnya 14 hari bekerja sebelum mesyuarat;

3) Kertas pembentangan digalakkan untuk dikemukakan kepada pihak urus setia sekurang-kurangnya tujuh (7) hari bekerja sebelum mesyuarat. Urus setia boleh memohon pihak yang berkenaan untuk menyediakan bahan pembentangan seperti yang berikut:

   a) Slaid atau kertas pembentangan atau kedua-duanya disediakan dalam bentuk salinan lembut (*soft copy*); dan

   b) Menyediakan ringkasan eksekutif (sekiranya perlu). Ringkasan eksekutif disediakan bagi kertas pembentangan melebihi 15-muka surat (tidak termasuk lampiran).

   c) Mengadakan sesi pramesyuarat untuk membincangkan kertas-kertas yang akan dibentangkan (sekiranya perlu);

   d) Memuat naik kertas pembentangan dan lain-lain dokumen seperti fail-fail agenda dan slaid untuk makluman ahli mesyuarat menerusi Sistem eMeeting; dan

e) Kertas pembentangan perlu diedarkan kepada ahli mesyuarat dalam tempoh lima (5) hari bekerja sebelum mesyuarat setelah dipersetujui dalam pramesyuarat bersama Pengerusi Mesyuarat.

(iv) Mendapatkan Maklum Balas Bagi Mesyuarat Lepas

1) Pihak urus setia hendaklah memastikan agar maklum balas bagi mesyuarat lepas diperoleh daripada PTJ/Pegawai yang berkenaan agar status tindakan yang telah dan akan diambil dimaklumkan dalam mesyuarat yang akan datang. Laporan maklum balas akan dijana daripada minit mesyuarat yang disediakan dan ahli juga boleh terus mengemas kini maklum balas melalui emel kepada Setiausaha atau Sekretariat. Pengerusi Mesyuarat boleh memantau status maklum balas oleh ahli dan memberi ulasan melalui Setiausaha atau Sekretariat.

(v) Menghantar Jemputan Mesyuarat

1) Urus setia hendaklah menghantar jemputan mesyuarat melalui edaran surat / emel sekurang-kurangnya tujuh (7) hari bekerja sebelum mesyuarat diadakan. Jemputan ini hendaklah mengandungi maklumat-maklumat asas seperti yang berikut:

a) Nama mesyuarat;

b) Tarikh dan tempat mesyuarat;

c) Masa mula

d) Nama dan jawatan Pengerusi Mesyuarat;

e) Agenda mesyuarat; dan

f) Pernyataan yang memaklumkan sama ada ahli yang dijemput dibenarkan menghantar wakil. Sekiranya dibenarkan, nama dan jawatan wakil hendaklah dinyatakan semasa pengesahan kehadiran.

(vi) Mengadakan Perbincangan Sebelum Mesyuarat

1) Perbincangan antara Pengerusi Mesyuarat dengan urus setia hendaklah diadakan untuk menetapkan kandungan perutusan pengerusi, meneliti maklum balas yang diterima serta mengenal pasti tindakan susulan yang perlu dilakukan. Urus setia hendaklah memastikan perkara-perkara berikut diberikan perhatian oleh Pengerusi Mesyuarat:

a) mematuhi waktu mesyuarat bermula dan tamat agar tempoh mesyuarat yang diperuntukkan dapat dioptimumkan;

b) memastikan semua perkara dalam agenda dibincangkan; dan

c) merumuskan perkara-perkara utama yang telah dipersetujui sebelum mesyuarat berakhir.

2) Norma kerja yang digalakkan untuk mengadakan perbincangan adalah dalam tempoh tiga (3) hingga tujuh (7) hari bekerja sebelum mesyuarat. Norma bagi mesyuarat utama Universiti adalah seperti berikut;

- Pra LPU – tujuh hari (7) sebelum Mesyuarat diadakan.
- Lain-lain mesyuarat – bergantung kepada Pengerusi Mesyuarat

(vii) Mengesahkan Kehadiran

1) Ahli mesyuarat dikehendaki membuat pengesahan kehadiran mesyuarat kepada pihak urusetia/setiausaha mesyuarat. Urus setia seterusnya akan menyediakan senarai kehadiran mesyuarat serta mencatat kehadiran wakil kepada ahli mesyuarat atau pegawai lain yang turut hadir. Senarai ini hendaklah disediakan dalam tempoh sekurang-kurangnya satu (1) hari bekerja sebelum mesyuarat diadakan. Senarai ini akan digunakan sebagai rekod kehadiran bagi tujuan penyediaan minit mesyuarat.

(viii) Memastikan Persediaan Kemudahan-Kemudahan Bilik Mesyuarat

1) Urus setia hendaklah memastikan bilik mesyuarat disediakan mengikut keperluan mesyuarat seperti yang berikut:

a) Menentukan bilik mesyuarat dalam keadaan bersih dan kemas;

b) Menyediakan tempat duduk yang mencukupi dan menyusun tanda nama Pengerusi Mesyuarat dan ahli mesyuarat (sekiranya perlu);

c) Memastikan alat kelengkapan mesyuarat seperti perakam suara, mikrofon, komputer, projektor, skrin, *slide controller* dan peralatan lain berfungsi dengan baik; dan

d) Memastikan juruteknik mudah dihubungi sekiranya berlaku sebarang masalah teknikal.

2) Urus setia perlu berada dalam bilik mesyuarat sekurang-kurangnya 30 minit sebelum mesyuarat bermula.

(ix) Menangguh atau Membatalkan Mesyuarat

1) Sekiranya berlaku penangguhan atau pembatalan mesyuarat, perkara-perkara berikut perlu diambil perhatian oleh urus setia:

a) Memaklumkan segera kepada semua ahli mesyuarat berhubung pembatalan mesyuarat melalui emel atau telefon;

b) Memastikan tempahan bilik mesyuarat, peralatan dan kemudahan dibatalkan.

6.3. PERINGKAT II: TINDAKAN SEMASA MESYUARAT

6.3.1. Urus setia bertanggungjawab memastikan perkara-perkara yang berikut dilaksanakan semasa mesyuarat:

(i) Mengemas kini kehadiran ahli mesyuarat semasa mesyuarat berlangsung.

(ii) Memastikan mesyuarat dijalankan mengikut agenda yang telah ditetapkan.

(iii) Memastikan semua ahli mesyuarat mendapat maklumat yang tepat dan terkini berhubung kertas kerja pembentangan.

(iv) Merekod perkara-perkara yang dibincangkan dalam mesyuarat bagi tujuan penyediaan minit mesyuarat.

6.4. PERINGKAT III: TINDAKAN SELEPAS MESYUARAT

6.4.1. Selepas mesyuarat diadakan, tindakan-tindakan berikut perlu dilaksanakan oleh urus setia mesyuarat.

(i) Menyediakan Minit Mesyuarat

a) Penulisan minit mesyuarat hendaklah ringkas, tepat, dan padat serta laras bahasanya bersifat formal.

b) Antara perkara yang perlu dititikberatkan dalam minit mesyuarat adalah:

i. Senarai kehadiran ahli mesyuarat disusun mengikut kekananan jawatan;

ii. Perkara-perkara penting yang dibincangkan dalam mesyuarat disusun mengikut tajuk dan perkara;

iii. Keputusan-keputusan yang dibuat hendaklah dicatat dengan jelas;

iv. Tindakan-tindakan susulan yang perlu diambil;

v. Menentukan pihak yang perlu mengambil tindakan susulan; dan

vi. Sekiranya terdapat butiran pembentangan kertas, urus setia hendaklah merekodkan perkara-perkara seperti yang berikut:

- Tajuk kertas pembentangan;
- Pihak yang menyediakan kertas pembentangan;
- Tujuan utama kertas pembentangan berkenaan disediakan;
- Isu-isu penting yang dibangkitkan dalam kertas pembentangan;
- Pandangan/ulasan ahli mesyuarat berkenaan isu yang dibangkitkan dalam kertas pembentangan;
- Keputusan mesyuarat terhadap kertas pembentangan.

c) Format Teknikal

- Pada asasnya, penulisan minit mesyuarat perlu menepati format teknikal minit mesyuarat seperti yang berikut:

(i) Jenis Fon (Font) : Arial

(ii) Saiz Fon (Font) : Minimum 12

(iii) Langkau Antara Barisan : Minimum 1.15

(iv) Kedudukan Teks : Justified

(v) Istilah Bahasa Inggeris : *Italic* (Sekiranya minit mesyuarat disediakan dalam Bahasa Melayu)

d) Struktur Minit Mesyuarat

- Struktur minit mesyuarat perlulah berpandukan agenda dan turutan mesyuarat seperti yang berikut:

(i) Senarai Kehadiran;

(ii) Perutusan Pengerusi;

(iii) Pengesahan Minit Mesyuarat;

(iv) Perkara-Perkara Berbangkit;

(v) Perbincangan;

(vi) Pembentangan Kertas;

(vii) Hal-Hal Lain; dan

(viii) Penutup.

e) Setiap perkara yang dibincangkan hendaklah diikuti dengan catatan yang menunjukkan sama ada tindakan diperlukan,

perhatian atau untuk makluman sahaja. Struktur minit mesyuarat secara manual adalah seperti di **Lampiran A .**

f) Minit mesyuarat yang berkualiti perlu menepati ciri-ciri sistematik, tepat, padat dan kemas. Format penyediaan minit mesyuarat akan membantu urus setia menyediakan minit dalam bentuk yang mudah difahami oleh ahli mesyuarat.

g) Minit mesyuarat perlu disiapkan dan dikemukakan kepada Pengerusi Mesyuarat untuk kelulusan dalam tempoh tiga (3) hari bekerja. Pengerusi Mesyuarat boleh menyemak dan meluluskan minit mesyuarat sebelum diedarkan secara dalam talian untuk pengesahan ahli mesyuarat.

h) Minit-minit mesyuarat khas mana-mana jawatankuasa hendaklah disahkan dalam Mesyuarat Biasa yang berikutnya.

i) Selepas minit-minit bagi sesuatu mesyuarat Lembaga disahkan menurut Peraturan ini, maka tiada sesuatu bantahan boleh dibuat sama ada berkenaan apa-apa kandungan minit-minit mesyuarat tersebut atau berkenaan sah atau tidaknya mesyuarat yang berkaitan itu.

j) Sekiranya terdapat keperluan untuk mendapatkan keputusan dengan segera atas sesuatu perkara penting, maka dengan persetujuan Pengerusi mana-mana jawatankuasa (LPU/JPU/Senat atau JK Khas LPU), perkara itu boleh dibuat secara kertas kerja secara edaran kepada ahli-ahli untuk mendapatkan kelulusan mereka. Ahli-ahli hendaklah diberi masa selama tujuh (7) hari bekerja untuk mengemukakan maklum balas kepada Setiausaha/ Urusetia samada bersetuju, berkecuali atau tidak bersetuju atas

perkara secara edaran tersebut. Setiap keputusan bagi perkara yang dibuat secara edaran hendaklah dilaporkan dalam Mesyuarat Biasa yang berikutnya.

(ii) Mengedarkan Minit Mesyuarat

a) Minit mesyuarat berserta format/borang maklum balas hendaklah diedarkan melalui atas talian / menerusi emel kepada ahli mesyuarat PTj / Pegawai Yang bertanggungjawab selewat-lewatnya empat belas (14) hari bekerja selepas pengesahan minit mesyuarat dibuat atau tertakluk kepada kelulusan atau arahan daripada Pengerusi mesyuarat atau jawatankuasa.

(iii) Mengedar dan Mendapatkan Maklum Balas Mesyuarat

a) Urus setia hendaklah mendapatkan maklum balas daripada ahli mesyuarat. PTj/Unit UMK yang bertanggungjawab melaksanakan keputusan mesyuarat hendaklah menghantar maklum balas kepada urus setia dengan menggunakan format di **Lampiran B** yang mengandungi perkara-perkara berikut:

1) Keputusan Minit Mesyuarat
   - Urus setia menyenaraikan keputusan mesyuarat seperti mana tercatat dalam minit mesyuarat berserta pihak yang bertanggungjawab untuk mengambil tindakan terhadap keputusan mesyuarat.

2) Maklum Balas
   - Ahli mesyuarat atau pihak yang bertanggungjawab perlu mengemukakan status terkini tindakan yang telah dilaksanakan.

(iv) Merekod dan Menyimpan Minit Mesyuarat

a) Sistem eMeeting mempunyai fungsi untuk menyimpan minit mesyuarat. Pada masa yang sama, urus setia mesyuarat juga perlu memastikan minit mesyuarat direkodkan secara teratur dalam sistem pemfailan UMK mengikut tata cara semasa bagi memudahkan pengawalan dan pengesanan dokumen.

(v) Merekod Nota Catatan Menghadiri Mesyuarat

a) Pihak Pengurusan Universiti telah bersetuju supaya mana-mana staf yang diarahkan atau dinamakan sebagai wakil Naib Canselor atau organisasi atau mana-mana ketua jabatan dalam menghadiri mesyuarat-mesyuarat penting dikehendaki untuk mengemukakan laporan berdasarkan kepada format Nota Catatan Menghadiri Mesyuarat. Pengisian laporan yang perlu dikemukakan tersebut adalah berdasarkan kepada skop yang dinyatakan seperti di **Lampiran C.** Format ini boleh dimuat turun daripada portal eComm UMK.

7. PEMAKAIAN

7.1. Panduan ini terpakai kepada semua jenis mesyuarat dalam UMK.

8. PEMBATALAN

8.1. Panduan ini akan menggantikan pekeliling/panduan yang telah dikeluarkan oleh UMK sebelum ini

9. TARIKH BERKUAT KUASA

9.1. Panduan ini berkuat kuasa mulai tarikh ianya dikeluarkan.

10. RUJUKAN

10.1. Pekeliling Transformasi Pentadbiran Awam Bilangan 2 Tahun 2018 (MyMesyuarat : Ekosistem Pengurusan Mesyuarat Era Digital) yang dikeluarkan oleh MAMPU.

10.2. Peraturan Universiti Malaysia Kelantan (Garis Panduan Tadbir Urus Lembaga Pengarah) 2015

10.3. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan1 Tahun 1993 (Panduan Mengenai Mesyuarat Pagi) yang dikeluarkan pada 2 Januari 1993.

10.4. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 2 Tahun 1991 (Panduan Pengurusan Mesyuarat dan Urusan Jawatankuasa-Jawatankuasa Kerajaan) yang dikeluarkan pada 1 April 1991.

SENARAI SEMAK KEPERLUAN MESYUARAT

(Catatkan Nama Mesyuarat)

Bil. ..... Tahun .....

Tarikh (Hari) :
Masa : Mula-Tamat
Tempat :
Pengerusi :

Tempahan Logistik

Nama Bilik Mesyuarat

- Tempat

Peralatan ICT

- Komputer riba
- Projektor
- Keperluan- Keperluan lain (Nyatakan)

Makan/Minum

- Minum pagi
- Makan tengah hari
- Minum petang
- Lain-lain (nyatakan)

Urus setia perlu memastikan peralatan telah diuji cuba sebelum mesyuarat. Urus setia perlu memastikan makanan dan minuman tersedia sekurang-kurangnya setengah jam sebelum waktu hidangan

Pengangkutan (jika berkaitan)

- Barang-barang keperluan mesyuarat
- Urus setia
- Ahli mesyuarat
- Kad keselamatan
- Keperluan parkir khas

Keperluan di Bilik Mesyuarat

- Tanda nama ahli mesyuarat
- Perakam suara
- Peralatan menulis
- Senarai kehadiran ahli mesyuarat mengikut kekananan
- Dokumen mesyuarat
- Lain-lain peralatan mengikut keperluan

Penyediaan susunan kekananan ahli mesyuarat

- Senarai ahli mesyuarat
- Senarai jemputan
- Senarai kehadiran semasa
- Susun atur kedudukan ahli-ahli mesyuarat.

LAMPIRAN A

STRUKTUR MINIT MESYUARAT

(Catatkan Nama Mesyuarat)
Bil. ..... Tahun .....

Tarikh :
Masa : (Masa mula dan masa tamat mesyuarat)
Tempat :

Hadir
Senarai nama ahli yang menghadiri mesyuarat berkenaan, bermula dengan nama Pengerusi Mesyuarat. Susunan nama hendaklah mengikut kekananan.

Hadir Bersama
Senarai nama pegawai yang bukan merupakan ahli mesyuarat tetapi dijemput khas untuk menghadiri mesyuarat atau telah turut serta menghadiri mesyuarat. Susunan nama hendaklah mengikut kekananan.

Urus Setia
Senarai nama pegawai yang menjadi urus setia mesyuarat. Susunan nama hendaklah mengikut kekananan.

Perutusan Pengerusi
Ruangan yang mengandungi catatan mengenai perkara-perkara penting yang telah dibangkitkan oleh Pengerusi Mesyuarat. Perkara perkara penting ini tidak semestinya dibangkitkan oleh Pengerusi Mesyuarat pada awal mesyuarat. Ia mungkin dibangkitkan semasa mesyuarat membincangkan perkara-perkara berbangkit atau semasa membincangkan kertas-kertas kerja atau di akhir mesyuarat.

Pengesahan Minit Mesyuarat
Catatan keputusan minit mesyuarat yang lepas, iaitu sama ada disahkan tanpa pindaan atau disahkan tertakluk kepada pindaan-pindaan tertentu. Jika ada pindaan, nyatakan pindaan-pindaan berkenaan.

Perkara-Perkara Berbangkit

- Ruangan ini mengandungi catatan mengenai perkara-perkara yang dibangkitkan di dalam mesyuarat yang lepas;
- Tajuk utama perkara berbangkit yang dibincangkan hendaklah dicatatkan. Untuk memudahkan rujukan dibuat, muka surat dan perenggan minit mesyuarat lepas membincangkan perkara yang sama hendaklah dicatatkan; dan

- Jika perkara-perkara berbangkit itu masih memerlukan tindakan, catatkan juga agensi atau pegawai yang perlu mengambil tindakan.

Perbincangan
Ruangan ini merekodkan perkara-perkara baharu yang dibincangkan oleh ahli-ahli mesyuarat. Susunan tajuk adalah mengikut agenda mesyuarat yang telah ditetapkan.

Pembentangan Kertas Kerja
Bagi mesyuarat tertentu, beberapa kertas kerja dibentangkan untuk perbincangan. Format penyediaan Kertas Kerja Pembentangan adalah seperti di Lampiran .Perkara yang perlu direkodkan di dalam ruangan ini ialah:

- Tajuk kertas kerja berkenaan;
- Nama pegawai yang menyediakan/menyemak/memperakukan kertas kerja berkenaan;
- Tujuan utama kertas kerja berkenaan disediakan;
- Isu-isu penting yang dibangkitkan di dalam kertas kerja berkenaan;
- Pandangan/ulasan ahli-ahli mesyuarat berkenaan isu-isu yang dibangkitkan di dalam kertas kerja berkenaan; dan
- Keputusan mesyuarat mengenai isu-isu yang dibangkitkan serta tindakan-tindakan susulan yang perlu diambil seterusnya.

Hal-Hal Lain
Ruangan ini merekodkan perkara-perkara lain yang tidak terkandung dalam agenda utama mesyuarat.

Penutup
Ruangan ini merekodkan perkara-perkara seperti:

- Masa mesyuarat tamat atau ditangguhkan;
- Ucapan terima kasih daripada Pengerusi Mesyuarat; dan
- Catatan mengenai tarikh mesyuarat yang akan datang jika tarikhnya telah ditentukan.

LAMPIRAN B

FORMAT MAKLUM BALAS MINIT MESYUARAT DARIPADA PTJ/FAKULTI

Contoh

BIL	KEPUTUSAN	MAKLUM BALAS
1.	Mesyuarat bersetuju meluluskan cadangan menggunapakai Pekeliling Perkhidmatan 99 Tahun 2019 Pengurusan Sumber Manusia **Tindakan : Pejabat Pendaftar**	Satu Pekeliling Pentabiran telah dikeluarkan bertajuk Pengurusan Sumber Manusia dan hebahan menerusi emel UMK telah dibuat pada 22 April 2019
2.	Mesyuarat bersetuju memperakukan pemakaian tatacara perolehan seperti yang terkandung dalam Pekeliling Perbendaharaan Kementerian Kewangan Malaysia **Tindakan : Bendahari**	Satu Kertas Kerja berkaitan akan dibentangkan dalam Mesyuarat LPU yang akan datang.

LAMPIRAN C

FORMAT NOTA CATATAN MENGIKUT TURUTAN

1. Nama Mesyuarat:

2. Tarikh:

3. Tujuan dan Skop Mesyuarat:

4. Kehadiran:

   (Sila nyatakan beberapa yang terpenting sahaja)

5. Perkara Penting Perbincangan:

6. Dapatan/Keputusan/Persetujuan:

7. Rumusan dan Tindakan Susulan:

   (Sila nyatakan kepentingannya kepada organisasi)

8. Disediakan oleh & tandatangan:

9. Tarikh:

LAMPIRAN B

KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 1 TAHUN 2021

LARANGAN PENGGUNAAN TELEFON BIMBIT, PERALATAN KOMUNIKASI DAN SEGALA PERALATAN ELEKTRONIK YANG MAMPU MERAKAM MAKLUMAT DALAM MESYUARAT PENTING KERAJAAN

JABATAN PERDANA MENTERI

28 April 2021

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Suruhanjaya
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
PRIME MINISTER'S DEPARTMENT
Setia Perdana 8, Kompleks Setia Perdana
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
MALAYSIA

Telefon : 603-8872 3333
Faks : 603-8888 3755
Emel : jpm@jpm.gov.my
Web : http://www.jpm.gov.my

Rujukan Kami: KPKK(R)100-1/5/4 Jld. 2 (31)
Tarikh: 28 April 2021

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Suruhanjaya
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 1 TAHUN 2021

LARANGAN PENGGUNAAN TELEFON BIMBIT, PERALATAN KOMUNIKASI DAN SEGALA PERALATAN ELEKTRONIK YANG MAMPU MERAKAM MAKLUMAT DALAM MESYUARAT PENTING KERAJAAN

1. TUJUAN

Pekeliling ini bertujuan menarik perhatian semua Ketua Setiausaha Kementerian, Ketua Jabatan Persekutuan, Setiausaha

Suruhanjaya, YB Setiausaha Kerajaan Negeri, Pihak Berkuasa Berkanun Persekutuan dan Negeri serta Pihak Berkuasa Tempatan untuk menguatkuasakan larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dalam Mesyuarat penting Kerajaan.

2. LATAR BELAKANG

2.1 Penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat menjadi satu keperluan semasa sebagai medium perhubungan yang pantas dan berkesan di Agensi Kerajaan. Namun begitu, penggunaannya secara tidak terkawal dalam Agensi Kerajaan boleh mendatangkan risiko ketirisan maklumat yang membahayakan pentadbiran Kerajaan.

2.2 Pekeliling ini dikeluarkan sebagai panduan kepada semua Ketua Jabatan untuk menyelaras ketetapan larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dalam mesyuarat yang membincangkan perkara rahsia rasmi berisiko tinggi di sesebuah Kementerian/Jabatan/Agensi Kerajaan.

2.3 Larangan ini bertujuan untuk mengekang dan menghalang sebarang penyalahgunaan sehingga boleh menjejaskan imej Kerajaan melalui penularan atau penyebaran maklumat rahsia rasmi sebelum sesuatu keputusan rasmi dikeluarkan.

2.4 Perenggan 130, Arahan Keselamatan (Semakan dan Pindaan 2017) memberi kuasa kepada Ketua Jabatan menentukan zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat.

2.5 Sejak kebelakangan ini berlaku beberapa kes pendedahan dan penyebaran maklumat rahsia rasmi dan berisiko tinggi melalui telefon bimbit yang melibatkan kepentingan awam. Keadaan sedemikian telah dijelaskan di perenggan 131, Arahan Keselamatan (Semakan dan Pindaan 2017).

3. TAFSIRAN

3.1 Tafsiran bagi maksud Pekeliling ini adalah seperti yang berikut:

3.1.1. **zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat** bermaksud:

i. ahli mesyuarat **dibenarkan** membawa telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dalam mesyuarat penting Kerajaan tetapi tidak dibenarkan menggunakannya seperti ketetapan berikut:

a. telefon dalam keadaan "*on*" tetapi ditetapkan dalam mod senyap atau "*airplane mode*";

b. telefon dimatikan; atau

c. telefon dalam keadaaan "*on*" tetapi tidak digunakan langsung dalam mesyuarat.

ii. ahli mesyuarat tidak dibenarkan membawa masuk telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dalam mesyuarat penting Kerajaan;

3.1.2. **Mesyuarat penting Kerajaan** bermaksud mesyuarat rasmi Kerajaan yang membincangkan perkara-perkara rasmi atau rahsia rasmi yang berisiko tinggi dan sensitif sehingga boleh menyebabkan ancaman kepada keselamatan dan pertahanan negara, menjejaskan ekonomi negara, menyebabkan kesusahan kepada pentadbiran Kerajaan dan menjatuhkan imej serta reputasi Kerajaan sekiranya didedahkan sebelum sesuatu keputusan mesyuarat dibuat; dan

3.1.3. **peralatan komunikasi** bermaksud apa-apa peralatan komunikasi yang berupaya untuk berkomunikasi, merakam sama ada dalam bentuk audio atau video, mengambil gambar (*capture*), mengimbas (*scan*), menyimpan dan/atau menyebar sesuatu maklumat rahsia rasmi.

4. PELAKSANAAN

4.1 Penetapan Zon Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi Dan Segala Peralatan Elektronik Yang Mampu Merakam Maklumat Dalam Mesyuarat Penting Kerajaan

4.1.1. Semua Ketua Jabatan atau pengerusi mesyuarat hendaklah menetapkan mana-mana Mesyuarat penting Kerajaan untuk dikuatkuasakan zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat kepada ahli-ahli mesyuarat seperti mana yang dinyatakan dalam perenggan 130, Arahan Keselamatan (Semakan dan Pindaan 2017).

4.1.2. Penetapan tersebut hendaklah mengambil kira risiko sekiranya sesuatu maklumat rasmi atau rahsia rasmi didedahkan melalui telefon bimbit atau peralatan komunikasi lain sebelum keputusan mesyuarat dikeluarkan secara rasmi.

4.1.3. Sebagai panduan, Mesyuarat penting Kerajaan boleh dikategorikan sepertimana berikut:

a. Mesyuarat Jemaah Menteri;

b. Mesyuarat Majlis Mesyuarat Kerajaan Negeri;

c. mesyuarat berkaitan keselamatan dan pertahanan Negara serta perhubungan antarabangsa yang memberi impak tinggi kepada pembuat keputusan Kerajaan;

d. mesyuarat pengurusan tertinggi sesuatu Kementerian/Jabatan/Agensi Kerajaan;

e. Mesyuarat Lembaga Perolehan Tender/Sebut Harga;

f. mesyuarat sesuatu operasi penguatkuasaan; dan

g. mana-mana mesyuarat lain yang penting dan boleh menjejaskan kelancaran fungsi pentadbiran Kerajaan sekiranya maklumat didedahkan tanpa kebenaran.

4.2 **Keperluan Bagi Menguatkuasakan Zon Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi Dan Segala Peralatan Elektronik Yang Mampu Merakam Maklumat**

4.2.1. Ketua Jabatan atau pengerusi mesyuarat hendaklah menentukan zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat. Penentuan ini adalah bergantung kepada risiko maklumat yang dibincangkan dalam sesuatu mesyuarat penting

Kerajaan seperti yang dinyatakan di perenggan 4.1.

4.2.2. Memastikan supaya peringatan berkaitan larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat hendaklah dimaklumkan di dalam surat jemputan mesyuarat bagi memastikan maklumat rahsia rasmi yang akan dibincangkan diberi perlindungan sepenuhnya.

4.2.3. Penetapan zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat hendaklah melalui notis larangan yang dipamerkan di dalam bilik mesyuarat dan/atau di depan pintu masuk bilik mesyuarat yang berkenaan.

4.2.4. Sebelum sesuatu mesyuarat bermula, peringatan berhubung larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat hendaklah dimaklumkan secara lisan oleh pengerusi mesyuarat kepada ahli-ahli mesyuarat terlibat.

4.3 **Notis Larangan**

4.3.1. Semua notis larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat di dalam bilik

mesyuarat diselaraskan secara seragam seperti berikut:

i. notis sekurang-kurangnya mempunyai saiz A4;

ii. notis hendaklah ditampal atau di pamer di tempat yang sesuai dan mudah dilihat atau dipaparkan melalui skrin komputer; dan

iii. perihal notis larangan hendaklah mempunyai latar belakang berwarna putih dan **bulatan tebal serta tanda palang tebal berwarna merah**. Notis larangan mengandungi perkataan **"DILARANG MENGGUNAKAN TELEFON BIMBIT, PERALATAN KOMUNIKASI DAN SEGALA PERALATAN ELEKTRONIK YANG MAMPU MERAKAM MAKLUMAT"** dengan berwarna hitam.

4.3.2. Jabatan boleh mencetak sendiri notis larangan seperti **contoh di Lampiran A**.

4.4. Kawalan dan Pematuhan Larangan

4.4.1. Sekiranya zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat di perenggan 3.1.1(i) ditetapkan oleh Ketua Jabatan di mana ahli-ahli mesyuarat **dibenarkan** membawa telefon dan

peralatan komunikasi lain dalam mesyuarat penting Kerajaan, maka pengerusi atau urus setia mesyuarat hendaklah:

i. memastikan ahli mesyuarat mematuhi peraturan larangan melalui notis larangan yang dipamerkan di dalam bilik mesyuarat tersebut;

ii. memantau sebarang aktiviti mencurigakan melibatkan penggunaan telefon bimbit atau peralatan komunikasi lain semasa mesyuarat sedang berlangsung;

iii. mengambil tindakan seperti berikut iaitu:

a. memberi peringatan larangan;

b. mengarahkan supaya semua telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dimatikan (*switch off*);

c. memberhentikan mesyuarat seketika sekiranya terdapat ahli mesyuarat yang menggunakan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat ;

d. merekodkan nama mana-mana ahli

mesyuarat yang menggunakan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat ketika mesyuarat sedang berlangsung; dan

e. mengambil tindakan sewajarnya berdasarkan budi bicara pengerusi sekiranya terdapat ahli mesyuarat yang gagal mematuhi larangan tersebut.

4.4.2 Sekiranya zon larangan penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat di perenggan 3.1.1(ii) ditetapkan oleh Ketua Jabatan di mana ahli-ahli mesyuarat **tidak dibenarkan** membawa masuk telefon bimbit dan peralatan komunikasi lain, berikut adalah tindakan yang perlu diambil iaitu:

i. urus setia mesyuarat hendaklah menyediakan peti/ bekas simpanan khas yang bersesuaian dan ditempatkan di luar bilik mesyuarat;

ii. urus setia mesyuarat hendaklah memastikan keselamatan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat yang berada dalam simpanannya;

iii. urus setia mesyuarat hendaklah merekodkan butiran pemilik telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat bagi mengelakkan berlakunya kesilapan penyimpanan; dan

iv. urus setia mesyuarat hendaklah memulangkan kembali telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat kepada pemilik sebenar selepas tamat sesuatu mesyuarat.

4.4.3 Semua ahli mesyuarat adalah tertakluk kepada larangan dan had penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat semasa mesyuarat sedang berlangsung di zon larangan yang dikuatkuasakan melalui notis larangan tersebut.

4.4.4 Ahli-ahli mesyuarat hendaklah mengisytiharkan dan menyerahkan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat kepada pihak urus setia mesyuarat untuk tujuan simpanan sebelum dibenarkan masuk ke dalam bilik mesyuarat.

4.4.5 Ketua Jabatan mempunyai kuasa sepenuhnya ke atas larangan yang dikuatkuasakan ini. Sekiranya terdapat pegawai atau kakitangan serta ahli-ahli mesyuarat

gagal untuk mematuhi larangan tersebut, tindakan sewajarnya hendaklah diambil. Jika terdapat sebarang aktiviti yang memudaratkan keselamatan dan bersalahan dengan Akta Rahsia Rasmi 1972 [*Akta 88*], maka Ketua Jabatan hendaklah membuat laporan ke Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia atau laporan kepada balai polis yang terdekat sekiranya disyaki suatu kesalahan jenayah telah berlaku.

5. PENGECUALIAN

Larangan ini tidak terpakai kepada mana-mana mesyuarat yang tidak berisiko tinggi.

6. TARIKH KUAT KUASA

Pekeliling ini berkuat kuasa mulai tarikh ia dikeluarkan.

7. PEMAKAIAN

Pekeliling ini terpakai kepada semua Kementerian, Jabatan, Badan Berkanun, Kerajaan Tempatan, Agensi Kerajaan di peringkat Persekutuan dan Negeri serta mana-mana orang, tribunal, badan, institusi atau pihak berkuasa yang diisytiharkan sebagai perkhidmatan awam melalui perintah oleh Menteri dalam Warta mengikut peruntukan Akta Rahsia Rasmi 1972 [*Akta 88*].

8. MAKLUMAT PERTANYAAN

Sebarang pertanyaan berhubung pekeliling ini dan pekeliling yang berkaitan, hubungi:

Ketua Pengarah Keselamatan Kerajaan
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Jabatan Perdana Menteri
Aras -1, 1 & 2, Blok B7
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI MOHD ZUKI BIN ALI)
Ketua Setiausaha Negara

LAMPIRAN A

ZON LARANGAN PENGGUNAAN TELEFON, PERALATAN KOMUNIKASI DAN SEGALA PERALATAN ELEKTRONIK YANG MAMPU MERAKAM MAKLUMAT

LAMPIRAN C

UNIVERSITI
MALAYSIA
KELANTAN

DASAR KESELAMATAN ICT

UNIVERSITI MALAYSIA KELANTAN

Ogos 2019 versi 1.1

[*bahagian muka surat ini sengaja dibiarkan kosong*]

ISI KANDUNGAN

SEJARAH DOKUMEN

TARIKH	EDISI	KELULUSAN	TARIKH KUATKUASA
MEI 2011	**1.0**	**JPICTU BIL 2/2011**	**07/05/2011**
OGOS 2019	**1.1**	**JPICTU BIL 1/2019**	**06/08/2019**

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat & Komunikasi (ICT) Universiti. Dasar ini juga menerangkan kepada semua pengguna di UMK mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Universiti. Dasar ini dibuat berdasarkan kepada **Pekeliling Am Bilangan 3 Tahun 2000** bertajuk **"Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"** dan **Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)** yang telah dikeluarkan oleh MAMPU.

OBJEKTIF

Dasar Keselamatan ICT Universiti diwujudkan untuk menjamin kesinambungan urusan Universiti dengan meminimumkan kesan insiden keselamatan ICT.

MATLAMAT

Matlamat utama Dasar Keselamatan ICT Universiti adalah tidak terhad seperti berikut: -

i. memastikan aset ICT dilindungi secukupnya dari perbuatan salahguna atau kecurian / kehilangan;

ii. meminimumkan risiko ke atas aset ICT

iii. memastikan kelancaran operasi harian aset ICT; dan

iv. melindungi kepentingan pihak-pihak bergantung kepada aset ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan dan aksesibiliti aset ICT.

SKOP

Dasar ini meliputi semua aset ICT yang digunakan seperti:-

i. <u>Maklumat</u>

Aset yang digunakan untuk menyokong tadbir urus perkhidmatan Universiti yang melibatkan media storan, prosesan atau penghantaran data, dan juga data itu sendiri. Aset Maklumat termasuk sistem-sistem aplikasi, sistem-sistem pengoperasian, perisian utiliti, sistem-sistem komunikasi, data (sama ada dalam bentuk mentah, ringkasan atau ditafsirkan) dan perkakasan yang berkaitan dengan komputer seperti pelayan, komputer mudah alih, perkakasan komunikasi dan lain-lain perkakasan yang digunakan untuk menyokong urusan perkhidmatan Universiti.

ii. <u>Komunikasi</u>

Gabungan perkakasan telekomunikasi, alat-alat transmisi, video elektronik dan perkakasan audio, perkakasan mengkod dan mentafsir kod, komputer peribadi, prosesan data atau sistem-sistem storan, sistem-sistem komputer, komputer pelayan, rangkaian-rangkaian komputer, alat-alat input/output dan penyambungannya, dan rekod-rekod komputer, program, software dan dokumentasi yang berkaitan yang menyokong perkhidmatan

komunikasi.

iii. Dokumentasi

Semua dokumentasi (manual dan prosedur) yang mengandungi maklumat berkaitan dengan spesifikasi teknikal (termasuk dan tidak terhad kepada kod sumber, struktur dan kamus data), penggunaan elektronik. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, transperencies, risalah dan slaid.

iv. Premis Komputer dan Komunikasi

Semua premis yang digunakan untuk menempatkan aset ICT i) – iii) di atas.

Dasar ini adalah terpakai oleh semua pengguna di UMK termasuk staf, pembekal, pakar runding dan pihak sumber luar yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Universiti.

PRINSIP-PRINSIP

Prinsip yang menjadi asas kepada Dasar Keselamatan ICT Universiti dan hendaklah dipatuhi adalah seperti berikut: -

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya dibenarkan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermaksud akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut

i. Klasifikasi Maklumat – hendaklah mematuhi "**Arahan Keselamatan Kerajaan**" perenggan 53, muka surat 15.;

ii. Tapisan Keselamatan Pengguna – siasatan yang menunjukkan tiada sebab atau faktor untuk menghalang kebenaran mengakses kategori maklumat tertentu;

b. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan / atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna / bidang tugas;

c. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT di bawah kawalannya. Tanggungjawab ini hendaklah dinyatakan dengan jelas sejajar dengan

tahap sensitiviti sesuatu aset ICT berkenaan.

d. Pengasingan

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara bahagian operasi dan rangkaian.

e. Pengauditan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit.;

f. Pematuhan

Dasar Keselamatan ICT Universiti hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT Universiti.;

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui penduaan dan mewujudkan pelan pemulihan bencana / kesinambungan perkhidmatan.; dan

h. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisma keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 01: DASAR KESELAMATAN ICT

Objektif	
Mengambil langkah-langkah persediaan bagi perlindungan keselamatan aset ICT dan mengurangkan impak akibat perlanggaran atau bencana yang berlaku.	
0101 Pelaksanaan Dasar	
Pelaksanaan Dasar ini akan dijalankan oleh Pengerusi JPICTU selaku Pengerusi Jawatankuasa Pemandu ICT Universiti (JPICTU) dibantu oleh staf CCI yang terdiri daripada:- a. Pengarah CCI; b. Pegawai Keselamatan ICT (ICTSO); c. Pentadbir Sistem ICT; dan d. semua Pegawai Teknologi Maklumat.	Pengerusi JPICTU
0102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna UMK (termasuk staf, pembekal, pakar runding dan sebagainya)	ICTSO
0103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT Universiti: - a. kenalpasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Universiti (JPICTU); a. perubahan yang dipersetujui oleh JPICTU hendaklah dimaklumkan kepada semua pengguna; dan b. dasar ini hendaklah dikaji semula sekurang-kurang sekali setahun (apabila perlu).	ICTSO
0104 Pemakaian Dasar	
Dasar Keselamatan ICT Universiti adalah terpakai kepada semua pengguna ICT UMK dan tiada pengecualian diberikan.	Pengarah ICT

0105 Kawalan Pindaan	
Objektif	
Mengemaskini Dasar Keselamatan ICT Universiti bagi memastikan keselamatan aset ICT selari dengan perubahan masa dan keperluan serta perkembangan teknologi ICT terkini.	
010501 Pindaan Kepada Dasar	
Berikut merupakan prosedur yang hendaklah diikuti untuk membuat sebarang pindaan kepada dasar.	Pengarah ICT / ICTSO

a. Sebarang pindaan yang hendak dibuat kepada Dasar Keselamatan ICT hendaklah dilakukan dengan menulis secara rasmi kepada Pengarah ICT atau ICTSO. Pindaan-pindaan tersebut akan dibawa ke mesyuarat JPICTU untuk diluluskan; b. Sebarang pindaan kepada Dasar Keselamatan mestilah dihebahkan kepada semua pengguna. Cara hebahan bolehlah dilakukan melalui risalah, pekeliling, e-mail, atau paparan di laman web Universiti; c. ICTSO adalah bertanggungjawab menyimpan semua pindaan dan memasukkan pindaan-pindaan tersebut ke dalam Dasar Keselamatan ICT Universiti; dan d. Dokumen ini adalah dikaji semula setiap enam bulan sekali oleh Pasukan Pengurusan Keselamatan ICT Universiti.	
010502 Pemberitahuan Pindaan	
Sebarang maklum balas, pertanyaan atau pindaan kepada dasar ini hendaklah diajukan kepada ICTSO: Nama : Pegawai Keselamatan ICT Universiti Alamat : Pusat Komputeran Dan Informatik Universiti Malaysia Kelantan, Karung Berkunci 36, Pengkalan Chepa, 16100 Kota Bharu, Kelantan. No. Telefon : +609 – 771 7117 No Fax : +609 – 771 7172 e-Mel : fadli@umk.edu.my	ICTSO

BAHAGIAN 02: PENGURUSAN KESELAMATAN ICT UNIVERSITI

0201 Struktur Organisasi Pengurusan Keselamatan ICT Universiti	
Objektif	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
020101 Pengerusi JPICTU	
Peranan dan tanggungjawab Pengerusi JPICTU adalah seperti berikut : a. memastikan semua pengguna memahami peruntukan- peruntukan di bawah Dasar Keselamatan ICT Universiti; b. memastikan semua pengguna mematuhi dan tertakluk kepada Dasar Keselamatan ICT Universiti; c. memastikan semua keperluan organisasi (sumber kewangan, staf dan perlindungan keselamatan) adalah mencukupi; d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Universiti; dan e. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Universiti;	JPICTU
020102 JPICTU	
Tugas dan tanggungjawab JPICTU adalah seperti berikut: a. menentukan halatuju keselamatan ICT Universiti b. membangun pelan dan dasar keselamatan ICT Universiti; c. menyenarai isu-isu keselamatan ICT mengikut keutamaan, yang dihadapi oleh Universiti; d. menyedia cadangan tindakan keselamatan ICT termasuk sumber yang diperlukan bagi melaksanakan cadangan- cadangan tersebut; e. menyenarai teknologi bagi menghadapi ancaman keselamatan ICT; f. membangun program latihan dan pembudayaan keselamatan ICT; dan g. membangun mekanisma menangani insiden bagi permasalahan keselamtan ICT.	Pengarah ICT
020103 Pengarah ICT	
Ketua Pusat Komputeran dan Informatik (CCI) adalah merupakan Pengarah ICT Universiti. Peranan dan tanggungjawab Pengarah ICT adalah seperti berikut : a. membantu Pengerusi JPICTU dalam melaksanakan tugas- tugas melibatkan keselamatan ICT; b. menentukan keperluan keselamatan ICT; c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; d. menentukan tindakan tatatertib yang perlu diambil ke atas pengguna yang telah dikenalpasti melanggar Dasar Keselamatan ICT Universiti; e. memastikan semua warga UMK memahami dan mematuhi Dasar Keselamatan ICT Universiti; f. mengkaji semula dan melaksana kawalan keselamatan ICT selaras dengan keperluan Universiti; g. menentukan kawalan akses semua pengguna terhadap aset ICT	Pengarah ICT

Universiti; h. melaporkan penemuan mengenai pelanggaran Dasar Keselamatan ICT kepada ICTSO; dan i. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Universiti.	
020104 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT ialah pegawai yang dilantik oleh Naib Canselor/Pendaftar/CIO untuk bertanggungjawab terhadap pembangunan, pelaksanaan dan pelarasan program keselamatan ICT di Universiti. Peranan dan tanggungjawab beliau adalah tidak terhad seperti berikut:- a. mengurus keseluruhan program-program keselamatan ICT Universiti; b. menguatkuasa Dasar Keselamatan ICT Universiti; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Universiti kepada semua pengguna; d. mewujud garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Universiti; e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindakan kepada pengurusan Universiti berdasarkan hasil enemuan dan menyediakan laporan mengenainya; g. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada Pengarah ICT; i. bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. menyiasat dan mengenalpasti pengguna yang melanggar Dasar Keselamatan ICT Universiti; dan k. menyedia dan melaksana program-program kesedaran mengenai keselamatan ICT.	ICTSO
020105 Pentadbir Sistem ICT	
Pegawai Teknologi Maklumat di Bahagian Aplikasi dan Bahagian Teknikal & Operasi merupakan Pentadbir Sistem ICT Universiti. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: - a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat, sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT Universiti; c. memantau aktiviti akses harian pengguna; d. mengenalpasti aktiviti-aktiviti tidak normal seperti e. pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. menyimpan dan menganalisas rekod jejak audit; dan g. menyediakan laporan mengenai aktiviti akses kepada pemilik maklumat berkenaan secara berkala.	CCI
020106 Pemilik Sistem	
Pemilik Sistem merupakan Pusat Tanggungjawab yang bertanggungjawab terhadap sesuatu sistem. Peranan Pemilik Sistem adalah seperti berikut:	Pemilik Sistem

a. memastikan sistem beroperasi dengan baik dan lancar; b. memastikan segala data dan maklumat di dalam system adalah tepat, lengkap dan boleh dipercayai; dan c. memastikan sistem telah dilengkapi dengan langkah-langkah keselamatan melalui semakan senarai kawalanakses dan sebagainya.	
020107 Kaunter Perkhidmatan Help Desk	
Peranan Kaunter Perkhidmatan Help Desk adalah tidak terhad seperti berikut:- a. menjadi tempat rujukan dan melaporkan sekiranya berlaku masalah dan isu-isu berkaitan insiden keselamatan ICT; dan b. menjadi Pusat Informasi Insiden Keselamatan ICT Universiti;	CCI
020108 Pengguna	
Pengguna adalah merupakan semua warga Universiti. Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT Universiti; b. mengetahui dan memahami implikasi keselamatan ICT serta kesan dari tindakannya; c. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat Universiti; d. melaksanakan langkah-langkah perlindungan seperti berikut: i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan maklumat tersebut tepat dan lengkap dari semasa ke semasa; iii. menentukan kesahihan dan kesediaan maklumat untuk digunakan; iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. e. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengarah ICT, ICTSO atau Pentadbir Sistem ICT dengan segera; f. menghadiri program-program kesedaran mengenai keselamatan ICT; g. bertanggungjawab ke atas aset ICT di bawah kawalannya; dan h. menandatangani surat akuan pematuhan Dasar Keselamatan ICT Universiti.	Warga UMK

0202 Pihak Ketiga	
Objektif	
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Akses kepada aset ICT Universiti perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. a. Dasar Keselamatan ICT Universiti; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; dan d. Hak Harta Intelek	Pengarah ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

Nota Rujukan a. Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk “Tatacara Penyediaan, Penilaian dan Penerimaan Tender” dan b. Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan”	

BAHAGIAN 03: PENGURUSAN ASET

0301 Akauntabiliti Aset	
Objektif	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Universiti.	
030101 Inventori Aset	
Semua aset ICT Universiti hendaklah direkodkan. a. Ini termasuklah mengenalpasti, mengkategorikan aset dan merekodkan maklumat seperti pemilik, lokasi dan sebagainya; dan b. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya	CCI, Warga UMK

0302 Pengelasan dan Pengendalian Maklumat	
Objektif	
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen **Arahan Keselamatan Kerajaan** seperti berikut : a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Warga UMK
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambilkira langkah-langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan memastikan maklumat adalah tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Warga UMK

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 04: KESELAMATAN SUMBER MANUSIA

0401 Keselamatan ICT Dalam Tugasan Harian	
Objektif	
Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Universiti.	
040101 Tanggungjawab Keselamatan	
Tanggungjawab Keselamatan. a. Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak; dan b. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam tugas harian.	Warga UMK
040102 Terma dan Syarat Perkhidmatan	
Terma dan syarat Perkhidmatan UMK adalah seperti berikut: - a. warga UMK yang akan dilantik hendaklah mematuhi: i. menandatangani surat akuan Pemantuhan Dasar Keselamatan ICT Universiti; dan ii. melepasi Tapisan Keselamatan. b. semasa perkhidmatan, warga UMK tertakluk kepada Surat Akujanji dan **Akta 605 – Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000**; dan c. memulangkan semua aset ICT di bawah kawalannya kepada UMK.	Warga UMK
040103 Perakuan Akta Rahsia Rasmi	
Warga UMK yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan **Akta Rahsia Rasmi 1972**.	Warga UMK

0402 Menangani Insiden Keselamatan ICT	
Objektif	
Meminimumkan kesan insiden keselamatan ICT	
040201 Pelaporan Insiden	
Insiden keselamatan ICT adalah perlu dilaporkan kepada ICTSO atau Pengurus ICT dengan kadar segera: - a. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. kata lalaun atau mekanisma kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan kesilapan komunikasi; e. berlaku percubaan menceroboh, penyelewangan dan insiden-insiden yang tidak tidak diingani.	Warga UMK

0403 Pendidikan	
Objektif	
Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT	
040301 Program Kesedaran Keselamatan ICT	
Program Kesedaran Keselamatan ICT a. Setiap pengguna di UMK perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka b. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT Universiti.	ICTSO

0404 Tindakan Tatatertib	
Objektif	
Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT Universiti.	
040401 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT Universiti akan dikenakan tindakan tatatertib berdasarkan **Akta 605 – Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000**.	Warga UMK

BAHAGIAN 05: KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan	
Objektif	
Mencegah akses fizikal yang dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.	
050101 Perimeter Keselamatan Fizikal	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal adalah berikut : - a. Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding, siling dan lantai; d. Mengadakan kaunter kawalan, kad pintar, kamera litar tertutup (CCTV) dan sebagainya; e. Menyediakan tempat atau bilik khas untuk pelawat; f. Mengadakan pagar dan lampu keselamatan serta meghadkan pintu keluar masuk; dan g. Mengadakan pengawal keselamatan samaada yang mempunyai kuasa atau tidak di bawah undang-undang dan dilengkapi dengan alat-alat keselamatan.	Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.
050102 Kawalan Masuk Fizikal	
Kawalan Masuk Fizikal hendaklah tidak terhad seperti berikut : a. Setiap staf di UMK hendaklah memakai atau mengenakan kad staf sepanjang waktu bertugas; b. Setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Pengawal Keselamatan; d. Hanya staf dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu jabatan.	Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.
050103 Kawasan Larangan	
Kawasan terperingkat ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang dibenarkan akses sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Akses kepada kawasan terperingkat hanya kepada pegawai-pegawai yang diberikan kuasa sahaja : a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas berkenaan selesai; dan c. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat	Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.

kebenaran daripada Pengerusi JPICTU	

0502 Keselamatan Kelengkapan	
Objektif	
Melindungi peralatan dan maklumat	
050201 Peralatan	
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO dan Pengarah ICT	Warga UMK
050202 Media Storan	
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar, Langkah-langkah pencegahan seperti berikut hednagklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d. Pergerakan media storan hendaklah direkodkan.	Warga UMK
050203 Kabel	
Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat terdedah. Langkah-langkah keselamatan yang perlu di ambil adalah seperti berikut : a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan c. Melindungi laluan pemasangan kabel sepenuhnya	CCI dan ICTSO

0503 Keselamatan Komunikasi & Operasi	
Objektif	
Meminimumkan risiko keselamatan akibat kegagalan kelengkapan beroperasi yang telah ditetapkan.	
050301 Penyelenggaraan	
Perkakasan hendaklah disenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti : a. Semua perkakasan yang disenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh disenggarakan oleh staf atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT berkenaan; dan e. Semua aktiviti penyelenggaraan perlu direkodkan di dalam borang harta modal.	CCI
050302 Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat	
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada kepada pelbagai risiko. Langkah-langkah berikut tidak terhad hendaklah diambil untuk menjamin keselamatan perkakasan : a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan Pengarah ICT dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Warga UMK
050303 Perkakasan di Luar Premis	
Bagi perkakasan yang dibawa keluar dari premis UMK, langkah-langah keselamatan hendaklah diadakan dengan mengambilkira risiko yang wujud di luar kawalan UMK : a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambilkira langah-langkah keselamatan yang bersesuaian.	Warga UMK
050304 Pelupusan	
Aset ICT yang akan dilupuskan hendaklah melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan UMK : a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran; dan b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan.	CCI
050306 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk	Warga UMK

bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja staf atau di paparan skrin apabila staf tidak berada di tempatnya : a. Gunakan kemudahan password screen saver atau log keluar apabila meninggalkan komputer; dan b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	

0504 Keselamatan Persekitaran	
Objektif	
Melindungi aset ICT Universiti dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian dan kemalangan.	
050401 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada **Pejabat Pembangunan & Pengurusan Infrastruktur (3PI)** Bagi menjamin keselamatan persekitaran, langkah-langkah berikut perlu diambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan sepertiICTSO perlindungan kebakaran atau kilat / petir hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	ICTSO
050402 Bekalan Kuasa	
Bekalan Kuasa : a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai; b. Peralatan sokongan seperti UPS (Uninterruptable Power Supply) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengarah ICT

050403 Prosedur Kecemasan	
Prosedur Kecemasan : **a.** Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada **Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam"**; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Universiti yang dilantik akan menggerakkan pasukan bantu mula kebakaran.	Pengarah ICT

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 06: PENGURUSAN OPERASI & KOMUNIKASI

0601 Pengurusan Prosedur Operasi	
Objektif	
Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
060101 Pengendalian Prosedur	
Pengendalian Prosedur adalah tidak terhad seperti berikut : a. semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal; b. setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c. semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan; dan d. semua staf UMK hendaklah mematuhi prosedur yang telah ditetapkan.	Pengarah ICT
060102 Kawalan Perubahan	
Kawalan Perubahan hendaklah tidak terhad seperti berikut : a. pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pengurus ICT terlebih dahulu; b. aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik komputer atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. semua aktiviti perubahan atau pengubahsuaian hendakalah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak.	CCI
060103 Prosedur Pengurusan Insiden	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambilkira kawalan-kawalan berikut :- a. mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. menyedia pelan kontigensi dan mengaktifkan pelan kesimbungan perkhidmatan; c. menyimpan jejak audit dan memelihara bahan bukti; dan d. menyediakan tindakan pemulihan segara.	ICTSO

0602 Perancangan dan Penerimaan Sistem	
Objektif	
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan system	
060201 Perancangan Kapasiti	
Perancangan Kapasiti hendaklah tidak terhad seperti berikut : a. kepasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. keperluan kapasiti ini perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO
060202 Penerimaan Sistem	
Semua sistem baru (termasuk sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT, ICTSO

0603 Perisian Berbahaya	
Objektif	
Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian seperti virus dan Trojan.	
060301 Perlindungan dari Perisian Berbahaya	
Perlindungan dari Perisian Berbahaya tidak terhad : a. memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti virus dengan penggunaan Intrusion Detection System (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. memasang dan menggunajan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. mengemaskini pattern anti virus sekerap yang mungkin (sekurang-kurangnya sekali sehari); e. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. memasukkan klusa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya; h. mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Warga UMK

0604 Housekeeping	
Objektif	
Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
060401 Penduaan	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti berikut perlu dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di off site. a. membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. memberi salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan c. menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada wakti kecemasan.	CCI
060402 Sistem Log	
a. mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaikpulih dengan segera; dan c. sekiranya wujud aktiviti-aktiviti tidak sah lain sepertu kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	CCI

0605 Pengurusan Rangkaian	
Objektif	
Melindungi maklumat dalam rangkaian dan infastruktur sokongan	
060501 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman keada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan (tidak terhad): a. tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan akses dan pengubahsuaian yang tidak dibenarkan; b. peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. akses kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi; e. firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi serta dikonfigurasi oleh pentadbir sistem; f. semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan UMK;	CCI

g. semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. memasang perisian Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) bagi mengensan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UMK; i. memasang Web Content Filter pada Internet Gateway untu menyekat aktiviti yang dilarang seperti termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; j. sebarang penyambungan rangkaian yang bukan di bawah kawalan UMK hendaklah mendapat kebenaran ICTSO; k. semua pengguna hanya dibenarkan menggunakan rangkaian UMK sahaja. Penggunaan modem adalah dilarang sama sekali; l. memastikan keperluan perlindungan ICT adalah bersesuai dan mencukupi bagi menyokkong perlindungan yang lebih optimum; dan m. sebarang penyambungan rangkaian daripada pihak ketiga (remote tunneling) ke dalam sistem rangkaian UMK hendaklah mendapat kebenaran ICTSO.	

0606 Pengurusan Media	
Objektif	
Melindungi aset ICT daripada kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
060601 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pengerusi JPICTU terlebih dahulu.	Warga UMK
060602 Prosedur Pengendalian Media	
Prosedur Pengendalian Media hendaklah : a. melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. menghadkan dan menentukan akses media kepada pengguna yang sah sahaja; c. menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. menyimpan semua media di tempat yang selamat; dan f. media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Warga UMK
060603 Keselamatan Sistem Dokumentasi	
Keselamatan Sistem Dokumentasi hendaklah: a. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. menyediakan dan memantapkan keselamatan sistem dokuementasi; dan c. mengawal dan merekodkan semua aktiviti akses sistem dokumentasi sedia ada.	Pentadbir Sistem ICT, ICTSO

0607 Keselamatan Komunikasi	
Objektif	
Melindungi aset ICT melalui sistem komunikasi yang selamat	
060701 Internet	
Tatacara penggunaan Internet adalah seperti berikut: a. laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengerusi JPICTU; b. bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengerusi JPICTU sebelum dimuat naik ke Internet; d. pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UMK; f. hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board. Walaubagaimana, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Pengerusi JPICTU terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan g. maklumat lanjut mengenai keselamatan Internet boleh dirujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"**.	Warga UMK
060702 Mel Elektronik	
Tatacara penggunaan Mel Elektronik tidak terhad seperti berikut : a. akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh UMK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh UMK; c. memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah sangat disarankan; f. pengguna hendaklah mengelak daru membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g. pengguna hendaklah mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpa mengikut tatacara pengurusan sistem fail eletronik yang telah ditetapkan;	Warga UMK

i. e-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan k. maklumat lanjut mengenai keselamatan e-mel boleh dirujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"**.	

BAHAGIAN 07: KAWALAN AKSES

0701 Dasar Kawalan Akses	
Objektif	
Memahami dan mematuhi keperluan dalam mencapai dan menggunakan aset ICT Universiti.	
070101 Keperluan Tugas	
Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan akses pengguna sedia ada.	CCI, ICTSO

0702 Pengurusan Akses Pengguna	
Objektif	
Mengawal akses pengguna ke atas aset ICT Universiti.	
070201 Akaun Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut perlu dipatuhi : a. akaun yang diperuntukan oleh Universiti sahaja boleh digunakan; b. akaun pengguna mestilah unik; c. akaun pengguna yang di wujud pertama kali akan diberi tahap akses paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Universiti. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. penggunaan akaun milik orang lain atau akauan yang dikongsi bersama adalah dilarang; f. Session time out perlu diaktifkan selepas tiada aktiviti berlaku pada sesuatu terminal selama 30 minit; dan g. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:- i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) bulan; ii. bertukar bidang tugas kerja; iii. bertukar ke agensi lain; iv. bersara; atau v. ditamatkan perkhidmatan.	Warga UMK

070202 Jejak Audit	
Jejak Audit a. Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi:- i. maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program digunakan; ii. aktiviti akses penggun ke atas sistem ICT sama ada secara sah atau sebaliknya; dan iii. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. b. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan mendapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsiaian yang tidak dibenarkan.	Pentadbir Sistem ICT

0703 Kawalan Akses Sistem dan Aplikasi	
Objektif	
Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk akses yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
070301 Sistem Maklumat & Aplikasi	
Akses sistem dan aplikasi di UMK adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan akses sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap akses dan sensitiviti maklumat yang telah ditetntukan; b. setiap aktiviti akses sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan akses bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. menghadkan akses sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau akses yang tidak sah; dan f. Akses sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walaubagaimana, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT, ICTSO

0704 Peralatan Komputer Mudah Alih	
Objektif	
Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.	
070401 Penggunaan Peralatan Komputer Mudah Alih	
Penggunaan Peralatan Komputer Mudah Alih a. merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan b. komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Warga UMK

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 08: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif	
Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian	
080101 Keperluan Keselamatan	
Keperluan Keselamatan. a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh menganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukan, sistem pemprosesan untuk menentukan output untuk memastikan data yang telah diproses adalah tepat; dan c. Sebaik-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO

0802 Kriptografi	
Objektif	
Melindungi kerahsiaan, integriti dan kesahihan maklumat	
080201 Penyulitan	
Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Warga UMK
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara eletronik.	Warga UMK
080203 Pengurusan Kunci	
Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Warga UMK

0803 Fail Sistem	
Objektif	
Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Kawalan Fail Sistem. a. Proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal akses ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan aufit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT

0804 Pembangunan dan Proses Sokongan	
Objektif	
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi	
080401 Kawalan Perubahan	
Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai.	Pentadbir Sistem ICT
080402 Hak Harta Intelek	
Semua pembangunan sistem maklumat dan aplikasi hendaklah dipastikan bahawa UMK akan menerima hak pemilikan Kod Sumber (Source code) dan hak harta intelek (Intellectual Property Right – IP) secara mutlak.	Pentadbir Sistem ICT

BAHAGIAN 09: PENGENDALIAN INSIDEN ICT

0901 Mekanisma Pelaporan	
Objektif	
Menyalurkan maklumat insiden ICT kepada GCERT untuk mendapat bantuan teknikal untuk tujuan penyelesaian atau pencegahan.	
090101 Insiden Keselamatan	
Insiden keselamatan boleh dikategori tidak terhad kepada kejadian-kejadian seperti berikut : a. percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (probing); b. serangan kod jahat (malicious code) seperti virus, trojan horse, worms dan sebagainya; c. gangguan yang disengajakan (unwanted disruption) atau halangan pemberian perkhidmatan (denial of service); d. menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (unauthorised access); dan e. pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.	ICTSO
090102 Tanggungjawab Pelapor	
Tanggungjawab pelapor adalah seperti berikut: a. mengurus tindakan ke atas insiden yang berlaku sehingga keadaan pulih; b. mengaktifkan Business Resumption Plan (BRP) jika perlu; c. menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan Undang-undang / Keselamatan; d. menentukan tahap keutamaan insiden; e. melaporkan insiden kepada GCERT; dan f. mengambil langkah pemulihan awal.	Pengarah ICT / ICTSO
090103 Kaedah Melapor	
Laporan boleh dibuat menggunakan kaedah-kaedah berikut : a. Mel Elektronik (e-mel) Alamat e-mel : gcert@mampu.gov.my b. Borang Pelaporan Insiden Borang boleh diperolehi di laman : http://gcert.mampu.gov.my c. Telefon hotline Nombor Telefon : +603 – 8888 3150 d. Faks Nombor faksimili : +603 – 8888 3286	ICTSO

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 10: PELAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan	
Objektif	
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Kesinambungan Perkhidmatan	
Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICTU dan perkara-perkara berikut perlu diberi perhatian: a. mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. mendokuemntasikan proses dan prosedur yang telah dipersetujui; d. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. membuat penduaan; dan f. menguji dan mengemaskini pelan sekurang-kurang setahun sekali.	ICTSO

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 11: PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan	
Objektif	
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Universiti.	
110101 Pematuhan Dasar	
Setiap pengguna di UMK hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Universiti dan undang-undang atau peraturan-peraturan lain yang berkaitan dikuatkuasakan. Semua aset ICT di UMK termasuk maklumat yang disimpan didalamnya adalah **Hak Milik Kerajaan** dan Pengerusi JPICTU berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Warga UMK
110102 Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di UMK : a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam"; g. Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender"; h. Surat Pekeliling Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan"; i. Akta Tandatangan Digital 1997; j. Akta Jenayah Komputer 1997; k. Akta Hak cipta (Pindaan) Tahun 1997; l. Akta Rahsia Rasmi 1972; m. Pekeliling Am Bilangan 1 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam"; dan n. Surat Pekeliling Am Bilangan 3 Tahun 2009 bertajuk "Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam".	Warga UMK

[*bahagian muka surat ini sengaja dibiarkan kosong*]

LAMPIRAN D

LAMPIRAN D

SURAT AKUAN AHLI MESYUARAT

TARIKH :
MASA :
TEMPAT :

i. Saya tidak akan melibatkan diri saya dalam mana-mana amalan rasuah dengan mana-mana pihak yang terlibat sama ada secara langsung atau tidak langsung dalam melaksanakan tanggungjawab saya sebagai ahli Mesyuarat _____

---

ii. Saya tidak akan bersubahat atau dipengaruhi oleh mana-mana pihak dalam melaksanakan tanggungjawab saya;

iii. Saya akan mengisytiharkan apa-apa kepentingan peribadi atau kepentingan terletak hak secarabertulis dan akan menarik diri daripada membuat sebarang keputusan;

iv. Sekiranya ada sebarang percubaan rasuah daripada mana-mana pihak, saya akan membuat aduan dengan segera ke pejabat Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) atau balai polis yang berhampiran. Saya sedar bahawa kegagalan saya berbuat demikian adalah satu kesalahan di bawah Akta Suruhanjaya Pencegahan Rasuah 2009 [Akta 694];

v. Saya tidak akan mendedahkan apa-apa maklumat sulit berkaitan keputusan mesyuarat ini kepada mana-mana pihak selaras dengan Akta Rahsia Rasmi 1972 [Akta 88];

Nama : .....

No. Kad Pengenalan : .....

Tandatangan : .....

Jawatan : .....

Tarikh : .....