SOP KESELAMATAN UMUM PEJABAT

POLITEKNIK MELAKA (PMK)

(Versi 1.0)

Disediakan oleh :

JK Keselamatan PMK

TUJUAN

SOP Keselamatan Umum Pejabat PMK ini dikeluarkan oleh JK Keselamatan PMK sebagai garis panduan kepada semua warga kerja Politeknik Melaka (PMK) bagi meningkatkan kualiti keselamatan perlindungan di Politeknik Melaka (PMK) dan hendaklah dibaca bersekali dengan Dokumen Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan. Selain itu, SOP ini juga merangkumi garis panduan bagi meningkatkan kualiti keselamatan ICT di Politeknik Melaka (PMK) dan hendaklah dibaca bersekali dengan Dokumen Dasar Keselamatan ICT Bagi Jabatan Pendidikan Politeknik dan Politeknik Malaysia yang dikeluarkan oleh Jabatan Pendidikan Politeknik.

SOP Keselamatan Umum Pejabat PMK dibahagikan kepada empat (4) bahagian utama iaitu :

A. **Keselamatan Fizikal,**

B. **Keselamatan Dokumen/Maklumat,**

C. **Keselamatan Peribadi/Personel dan**

D. **Keselamatan ICT.**

Bagi memudahkan pembacaan SOP ini beberapa akronim telah digunakan mengikut keterangan yang berikut:

PMK – Politeknik Melaka

UTM – Unit Teknologi Maklumat

PDRM – Polis Di Raja Malaysia

JBPM – Jabatan Bomba Dan Penyelamat Malaysia

ICT – Teknologi Maklumat

SOP – Standard of Procedure

KUKP – Ketua Unit Khidmat Pengurusan / PPT(K)

PAK – Pegawai Akaun (Kanan)

QRT – Quick Response Team

A. KESELAMATAN FIZIKAL

Kawalan Keselamatan PMK

1. Pihak pengurusan PMK telah menetapkan lokasi persekitaran yang diisytiharkan sebagai kawasan kampus PMK mengikut Peta Lokasi Kampus PMK seperti di *Lampiran 1.*
2. Kampus PMK dilengkapi dengan pagar elektronik berpalang di kedua-dua pintu masuk-keluar utama bagi mengawal pergerakan keluar-masuk ke kampus PMK.
3. Para pelawat perlu melapor diri di Pos Kawalan 1 – Pintu Masuk Utama PMK.
4. PMK telah mengadakan perkhidmatan kawalan keselamatan di 3 (TIGA) lokasi Pos Kawalan.
   - 4.1 Pos Kawalan 1 - Pintu Masuk Utama PMK
   - 4.2 Pos Kawalan 2 - Pintu Keluar PMK dan
   - 4.3 Pos Kawalan 3 - Pintu Masuk ke Dataran PMK.

5. Semua Pengawal Keselamatan di PMK perlu menjalankan tanggungjawab dan tugas rutin berikut :

   - 5.1 Mengawal dengan berpakaian seragam dilengkapi peralatan kawalan yang sewajarnya di tiga lokasi Pos Kawalan PMK.
   - 5.2 Mengawal laluan masuk, pergerakan pelawat dan kenderaan masuk-keluar kawasan kampus PMK
   - 5.3 Unit Khidmat Pengurusan (UKP) telah menyediakan Pas Pelawat dan borang yang perlu diisi oleh pelawat di Pos Kawalan 1 – Pintu Masuk Utama PMK.
   - 5.4 Pas Pelawat dan borang yang telah ditandatangani oleh pegawai yang ditemui perlu dipulangkan semula kepada Pengawal Keselamatan yang bertugas di Pos Kawalan 1.
   - 5.5 Pengawal Keselamatan perlu membuka pintu grill Aras Bawah yang ditetapkan oleh UKP sekitar jam 7.00 pagi dan menutup pintu tersebut selewat-lewatnya pada jam 7.00 petang.
   - 5.6 Penggunaan bilik kuliah, bengkel, bilik seminar dan fasiliti lain di luar waktu pejabat perlu menggunakan Borang Kebenaran Memasuki Premis Di Luar Waktu Pejabat dengan kelulusan Ketua Jabatan. Sesalinan borang tersebut perlu diserahkan kepada Pengawal Keselamatan.
   - 5.7 Pengawal Keselamatan perlu menjalankan rondaan mengikut spesifikasi kontrak perkhidmatan Syarikat Kawalan Keselamatan di seluruh kawasan kampus PMK sambil merakam 'Watchman Clock' pada setiap point yang ditetapkan dan mengawasi setiap pergerakan atau aktiviti yang berlaku di dalam atau luar premis secara fizikal;

5.8 Memeriksa dan menahan mana-mana individu atau kumpulan yang disyaki atau meragukan atau yang terlibat membawa/menyorokkan apa sahaja bentuk alatan membahayakan keselamatan semasa menjalankan rondaan di kawasan kampus PMK.

5.9 Menyediakan Laporan Keselamatan Harian / Mingguan bertulis secara lengkap dan kemas;

5.10 Melaporkan dalam bentuk Laporan Bertulis apa sahaja peristiwa dan kejadian yang tidak diingini atau cubaan pencerobohan atau kecurian kepada Pegawai Keselamatan Jabatan PMK dan PDRM; serta apa-apa kejadian kebakaran kepada JBPM; dan

5.11 Memastikan setiap Pos Kawalan sentiasa bersih dan bebas daripada segala bentuk atau peralatan yang tidak dibenarkan.

6. Pengawal Keselamatan di PMK perlu menjalankan tanggungjawab berikut ketika berlaku sebarang kecemasan/bencana di PMK:

6.1 Ketika kecemasan/bencana Pegawal Keselamatan perlu memastikan tiada kenderaan keluar atau masuk ke dalam kawasan kampus PMK

6.2 Ketiga-tiga pondok kawalan keselamatan perlu dikawal rapi oleh Pengawal Keselamatan dan mencegah/menahan sesiapa sahaja yang tidak berkenaan daripada memasuki kawasan kampus PMK.

6.3 Pengawal Keselamatan perlu memberi bantuan kepada *Pasukan Quick Response Team* PMK (QRT) apabila bantuan diperlukan.

Sistem Kunci Keselamatan

7. Pegawai Keselamatan Jabatan bersama semua pegawai lokasi yang bertanggungjawab perlu memastikan tingkap dan pintu diperkukuhkan dan dilengkapi dengan sistem kunci keselamatan mengikut keterangan berikut:

7.1 Semua Ketua Jabatan dan Ketua Unit di PMK perlu bertanggungjawab ke atas semua hal berkaitan dengan kunci dan anak kunci yang ada dalam simpanan masing-masing.

7.2 Semua Ketua Jabatan dan Ketua Unit di PMK perlu menyelenggara sebuah **Buku Rekod Kunci** masing-masing yang mengandungi senarai lengkap kesemua anak kunci yang digunakan dan mengemaskini serta menjalankan audit ke atas kunci-kunci tersebut.

7.3 KUKP perlu menyelenggara sebuah **Buku Rekod Kunci Pendua PMK** yang mengandungi senarai lengkap kesemua anak kunci pendua yang digunakan dan mengemaskini serta menjalankan audit ke atas kunci-kunci tersebut;

7.4 Ketua Jabatan, Ketua Unit dan KUKP perlu memastikan supaya anggota yang diamanahkan dengan kunci-kunci pendua keselamatan bertanggungjawab sepenuhnya terhadap keselamatan kunci-kunci tersebut;

7.5 Semua pegawai lokasi yang bertanggungjawab perlu memastikan supaya anak kunci di Jabatan/Unit termasuk kunci-kunci pendua di UKP adalah

dilabel mengikut sistem kod yang sesuai dan tepat. Hanya sistem kod sahaja yang digunakan untuk label anak kunci;

7.6 Semua pegawai lokasi yang bertanggungjawab perlu memastikan supaya anak kunci di Jabatan/Unit atau anak kunci pendua di UKP disimpan di dalam peti keselamatan berkunci dan hendaklah berada di lokasi pegawai bertanggungjawab bagi kunci-kunci tersebut;

7.7 Semua pegawai lokasi yang bertanggungjawab hendaklah mewujudkan **Buku Pergerakan Kunci** bagi merekodkan pergerakan anak kunci di Jabatan/Unit atau anak kunci pendua di UKP yang mengandungi butiran nama, waktu dan tandatangan pegawai yang meminjam kunci tersebut;

7.8 Semua pegawai lokasi yang bertanggungjawab perlu memastikan supaya semua anak kunci di Jabatan/Unit dan kunci pendua di UKP tidak boleh membuat salinan/pendua sama sekali tanpa kebenaran;

7.9 Pengarah PMK bersama KUKP dan PAK perlu memastikan supaya peti besi keselamatan diselenggara dengan betul. Nombor kombinasi peti besi hendaklah ditukar setahun sekali atau apabila anggota yang mengetahui nombor kombinasi telah bertukar/berhenti/bersara atau apabila telah mengesyaki bahawa nombor kombinasi peti besi tersebut telah diketahui umum;

7.10 Semua pegawai lokasi yang bertanggungjawab perlu memastikan supaya setiap anggota yang bertukar/berhenti/bersara menyerahkan semula kesemua anak kunci dalam simpanannya; dan

7.11 Semua pegawai lokasi yang bertanggungjawab perlu melaporkan segera jika berlaku kehilangan mana-mana anak kunci kepada Pegawai Keselamatan Jabatan yang akan menjalankan penyiasatan terhadap kehilangan tersebut dan seterusnya perlu mengemukakan laporan kepada Pegawai Keselamatan Kerajaan dalam masa 24 jam.

Keselamatan Parkir Kenderaan

8. Bagi memudahkan tindakan segera diambil oleh semua pihak, berikut adalah beberapa saranan penting yang perlu dipatuhi bagi mengelakkan halangan semasa sebarang kecemasan/bencana berlaku:

   8.1 Dilarang meletak kenderaan secara BERLAPIS *(Double Parking)* di perkarangan PMK pada setiap masa.

   8.2 Dilarang meletakkan motosikal di mana-mana kaki lima bangunan PMK.

   8.3 Dilarang meletakkan kenderaan di dalam petak kuning pili bomba dan petak OKU dan HYBRID/NGV di PMK.

Pemantauan Syarikat Kawalan Keselamatan

9. KUKP perlu memastikan pegawai bertugas bagi memantau operasi rutin Syarikat Kawalan Keselamatan dan tugas – tugas lain yang diperlukan dari aspek keselamatan oleh Pegawai Keselamatan Jabatan dan JK Keselamatan PMK.

Keselamatan Kerja Di Lapangan

10. KUPS perlu memastikan semua tenaga kerja di bawah jagaannya yang melibatkan mana-mana kerja rutin di lapangan (*site*) di sekitar PMK sentiasa mematuhi arahan-arahan keselamatan yang sewajarnya mengikut jenis tugas masing-masing agar sentiasa berada dalam keadaan selamat.
11. Semasa menjalankan tugas penyenggaraan harian, setiap tenaga di bawah UPS perlu melaporkan dengan segera kepada KUPS jika terdapat mana-mana elemen pelanggaran arahan keselamatan atau jika menemui apa sahaja elemen yang berbahaya kepada warga PMK di mana-mana lokasi.
12. KUPS perlu memberi keutamaan secara serius terhadap mana-mana aduan kerosakan oleh warga kerja yang didapati mempunyai elemen yang membahayakan keselamatan warga PMK.
13. KUPS perlu memastikan Taklimat Keselamatan dijalankan sebelum mana-mana pekerja kontrak luar PMK mula menjalankan tugas kali pertama mereka di PMK.

Alat Penggera Kebakaran Dan CCTV

14. Pemantauan CCTV di PMK adalah di bawah pengurusan UTM manakala pemantauan alat penggera kebakaran adalah di bawah UPS.
15. KUTM perlu memastikan pegawai bertugas bagi memantau status operasi peralatan dan output dari aspek keselamatan bagi setiap unit CCTV di PMK dari semasa ke semasa.

Sistem Pas Keselamatan staf

16. Pihak UTM adalah pihak yang bertanggungjawab mengeluarkan Pas Keselamatan kepada setiap warga kerja PMK berdasarkan kategori berikut;
    16.1 Pas Keselamatan Tetap :
        (a) Disediakan untuk semua staf PMK dan merupakan pas rasmi untuk kegunaan mereka yang bertugas di PMK;
        (b) Had akses pas ditetapkan mengikut lokasi penempatan pegawai dan kawasan tertentu yang dibenarkan sahaja;
        (c) Setiap anggota Jabatan adalah bertanggungjawab terhadap Pas Keselamatan Tetap masing-masing.
    16.2 Pas Keselamatan Sementara :
        (a) Disediakan bagi kegunaan pelatih yang menjalani latihan di PMK atau bagi kegunaan sementara pegawai yang melaporkan kehilangan Pas Keselamatan Tetap;
        (b) Had akses pas ditetapkan mengikut lokasi penempatan pegawai/pelatih sahaja;

(c) Setiap pengguna Pas Keselamatan Sementara hendaklah bertanggungjawab terhadap pas yang dipinjamkan dan dikehendaki memulangkan semula pas tersebut kepada UTM setelah tamat tempoh latihan/menerima Pas Keselamatan Tetap yang baru.

16.3 Pas Keselamatan Khas :

(a) Disediakan bagi kegunaan semasa kecemasan atau keperluan bagi tujuan tertentu seperti melaksanakan kerja penyelenggaraan/ kontrak di luar waktu pejabat;

(b) Pas Keselamatan ini dibenarkan untuk mengakses masuk ke lokasi jabatan/unit dan ianya terhad kepada 1 unit sahaja;

(c) Pengguna Pas Keselamatan Khas hendaklah bertanggungjawab terhadap pas tersebut dan dikehendaki memulangkannya semula dengan kadar segera ke UTM setelah selesai penggunaan.

17. Setiap anggota Jabatan/pelatih dikehendaki sentiasa memakai Pas Keselamatan sepanjang berada di kawasan kampus PMK.

18. Pas Keselamatan tersebut hendaklah diserahkan kepada UTM apabila pemegang kad berpindah ke jabatan lain, bersara pilihan, bersara wajib atau berhenti dari perkhidmatan kerajaan.

19. Kehilangan Pas Keselamatan hendaklah dilaporkan segera oleh pemegang kad di Balai Polis berdekatan dan menyerahkan sendiri sesalinan laporan kehilangan ke UTM bagi tujuan pembatalan akses.

20. Sesiapa yang menjumpai Pas Keselamatan hendaklah menyerahkannya kepada:

POLITEKNIK MELAKA,
NO. 2 JLN. PPM 10,
PLAZA PANDAN MALIM,
75250 MELAKA.

B. KESELAMATAN DOKUMEN/MAKLUMAT

Pengurusan Sistem Fail PMK

1. Sistem Pergerakan Fail seperti Kad Indeks/Sistem Doket atau lain-lain sistem hendaklah diwujudkan untuk mengesan dan merekodkan pergerakan fail bagi mengatasi masalah kehilangan fail. Sehubungan itu, perkara-perkara tersebut hendaklah dilaksanakan:

    1.1 Fail terperingkat, dokumen sebut harga/tender, soalan peperiksaan dan lain-lain dokumen terperingkat disimpan dalam Kabinet Keluli Berpalang dan Berkunci serta dimangga dengan padlock yang bermutu tinggi atau disimpan di dalam Bilik Kebal. Dokumen rasmi yang tidak terperingkat hendaklah disimpan dalam kabinet keluli yang berkunci atau Mobile Filling Cabinet yang berkunci:

    1.2 Hanya anggota yang telah menandatangani Lampiran D Akta Rahsia Rasmi 1972 dan lulus tapisan keselamatan sahaja dibenarkan menguruskan dokumen terperingkat

    1.3 Bilik Fail hendaklah dikunci pada setiap masa. Segala urusan hendaklah melalui Kaunter Bilik Fail sahaja. Notis "DILARANG MASUK TANPA KEBENARAN" hendaklah ditampal di pintu masuk Bilik Fail dan pintu di mana dokumen terperingkat disimpan. Hanya anggota yang bertugas di Bilik Fail sahaja dibenarkan memasuki bilik berkenaan;

    1.4 Penghantaran fail terperingkat hendaklah menggunakan **beg berkunci**;

    1.5 Dokumen/Fail Sulit atau Terhad yang hendak dibawa keluar daripada pejabat untuk tujuan rasmi hendaklah mendapat kebenaran dari Ketua Jabatan; dan

    1.6 Buku Rekod Keluar/Masuk Surat, Buku Despatch dan lain-lain buku yang berkaitan dengan urusan surat-menyurat hendaklah dikemaskini dan dipantau setiap masa bertujuan untuk mengesan jika berlaku sebarang kehilangan surat-menyurat.

Penggunaan Mesin Penyalin

2. Memastikan serta mengawasi penggunaan mesin penyalin terutama sekali apabila membuat salinan dokumen terperingkat.
   2.1 Seorang pegawai yang bertanggungjawab bagi mengawasi mesin-mesin penyalin hendaklah dilantik serta sebuah Buku Daftar hendaklah diadakan bagi merekodkan penggunaannya;
   2.2 Hanya anggota yang dibenarkan sahaja boleh ditugaskan untuk membuat salinan dokumen terperingkat;
   2.3 Memastikan jumlah salinan yang dibuat ialah jumlah yang diluluskan sahaja dan semua salinan yang rosak hendaklah dibinasakan;
   2.4 Semakan ke atas buku daftar hendaklah dibuat untuk menentukan semua salinan dokumen terperingkat adalah dibuat mengikut peraturan; dan
   2.5 Semua penyelewengan dan penyalahgunaan ke atas mesin penyalin hendaklah dilaporkan kepada Ketua Jabatan.

Penggunaan Telefon Bimbit

3. Penggunaan telefon bimbit tidak boleh sewenang-wenangnya digunakan ketika berurusan dengan dokumen sulit atau terhad. Sehubungan itu, semua warga kerja PMK tidak boleh mengambil sebarang gambarfoto atau merakam video mana-mana dokumen yang dikelaskan sebagai sulit atau terhad kecuali dengan arahan, kebenaran atau jika terdapat keperluan daripada pihak pengurusan.
4. Penggunaan telefon bimbit juga tidak dibenarkan kepada para pelawat bagi mengambil sebarang gambarfoto atau merakam video lokasi-lokasi tertentu kecuali dengan kebenaran atau jika terdapat keperluan daripada pihak pengurusan.

C. KESELAMATAN PERIBADI/PERSONEL

1. Setiap anggota yang dikehendaki akses kepada perkara-perkara terperingkat hendaklah menandatangani borang akuan Lampiran 'D' Akta Rahsia Rasmi 1972 seperti yang terkandung dalam Arahan Keselamatan. Borang tersebut juga dikehendaki ditandatangani setiap tahun untuk tujuan peringatan. Sehubungan itu, perkara-perkara berikut hendaklah dilaksanakan:

   1.1 Setiap anggota hendaklah menandatangani borang perakuan Lampiran 'E' seperti yang terkandung dalam Arahan Keselamatan sebelum berhenti/meninggalkan perkhidmatan Kerajaan;

   1.2 Setiap anggota yang terlibat dengan maklumat terperingkat Sulit/Terhad dikehendaki membuat Tapisan Keselamatan Kasar;

   1.3 Ketua Jabatan adalah bertanggungjawab menyelenggara fail yang mengandungi satu senarai lengkap dan kemaskini mengenai semua Jawatan Keselamatan Berjadual dan senarai pemegang jawatan tersebut; dan

   1.4 Ketua Jabatan hendaklah memastikan keputusan Tapisan Keselamatan anggota direkodkan dalam Buku Perkhidmatan anggota berkenaan.

D. KESELAMATAN ICT

1. Setiap warga kerja yang bertanggungjawab melaksanakan tugas serta program/aktiviti yang melibatkan ICT hendaklah mematuhi garis panduan yang ditetapkan bagi memastikan aset ICT PMK sama ada berbentuk peralatan mahupun maklumat sentiasa dilindungi, diperlihara dan terjamin dari segi integriti, kerahsiaan dan kesahihannya. Keselamatan ICT yang perlu diberi perhatian meliputi keselamatan fizikal dan maklumat terutamanya yang melibatkan peralatan mudah alih. Garis panduan yang perlu dipatuhi adalah seperti berikut:

    1.1 Semua warga PMK bertanggungjawab memastikan keselamatan aset Kerajaan dan peralatan ICT yang dimiliki di bawah jagaan dan kawalannya sentiasa dijaga dan berfungsi dengan sempurna;

    1.2 Bahan mudah terbakar hendaklah disimpan di luar kawasan aset ICT;

    1.3 Semua bahan berbentuk cecair perlu diletakkan di tempat bersesuaian dan jauh dari aset ICT;

    1.4 Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. Pengguna juga di larang menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan dan dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

    1.5 Komputer riba dan peralatan mudah alih hendaklah dikawal dengan rapi, disimpan dan dikunci di tempat yang selamat apabila tidak digunakan pada setiap masa. Ini termasuk ketika dalam simpanan di pejabat atau bertugas diluar pejabat atau di rumah. Pengguna dilarang keras meninggalkan komputer riba dalam kenderaan kerana ia boleh dikesan dengan alat khas oleh pihak yang tidak bertanggungjawab. Pengguna juga dinasihatkan tidak meninggalkan komputer riba di rumah jika tidak berada di rumah dalam tempoh masa yang panjang. Sebaliknya ia hendaklah disimpan dan dikunci di pejabat.

    1.6 Pengguna komputer riba hendaklah dikawal dengan Pengenalan Pengguna (User ID) atau Kata Laluan (password).

    1.7 Bagi perkakasan gunasama di jabatan/unit, aktiviti keluar masuk penggunaan peralatan hendaklah direkodkan dalam Daftar Pergerakan Harta Modal Dan Inventori(Kew PA-6) dan dipertanggungjawabkan kepada seorang warga kerja jabatan bagi mengesan jika berlaku kehilangan atau kerosakan. Oleh itu, aktiviti pinjaman dan pemulangan perkakasan ICT mestilah direkodkan dalam Kew PA-6. Peminjam bertanggungjawab memulangkan perkakasan yang dipinjam dan memastikan ia berada dalam keadaan sempurna sebagimana semasa ianya dipinjam. Sebarang

kerosakan dalam tempoh pinjaman hendaklah dimaklumkan semasa pengembalian.

1.8 Bagi pinjaman komputer riba, peminjam bertanggungjawab menghapuskan semua fail dokumen yang disediakan atau diwujudkan oleh mereka sebelum ia dikembalikan.

1.9 Perkakasan ICT yang dipinjam untuk kegunaan di luar pejabat terdedah kepada pelbagai risiko. Oleh itu, peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan berjawatan Ketua Jabatan / Unit. Ianya adalah tertakluk kepada tujuan yang dibenarkan sahaja. Pengguna dikehendaki mengisi Borang Kelulusan Permohonan Membawa Keluar Peralatan/Perisian ICT Daripada Jabatan dan diserahkan kepada Ketua Jabatan / Unit yang berkenaan.

1.10 Semua warga jabatan dilarang menggunakan komputer riba, thumb drive, CD, external hardisk dan mana-mana media komputer mudah alih untuk menyimpan maklumat terperingkat jabatan kecuali dengan kebenaran Ketua Jabatan atau Pengurusan Tertinggi jabatan.

1.11 Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Oleh itu, konsep *clear desk* dan *clear screen* hendaklah diamalkan di mana warga jabatan tidak meninggalkan bahan-bahan sensitif terdedah sama ada atas meja atau paparan skrin komputer apabila tidak berada di tempat masing-masing walaupun seketika. Langkah-langkah berikut hendaklah diambil;

(a) Log keluar komputer apabila meninggalkan komputer
(b) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail berkunci: dan
(c) Dokumen-dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak.

1.12 Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/Pegawai yang diberi kuasa;

1.13 Semua pengguna dibenarkan menggunakan rangkaian yang disediakan di PMK sahaja. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;

1.14 Pengguna mesti memastikan perisian antivirus di komputer masing-masing sentiasa aktif (activated) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan;

1.15 Semua pengguna dilarang sama sekali melakukan sebarang aktiviti yang melanggar tata cara penggunaan internet seperti mengakses maklumat terlarang, memuat naik, memuat turun, menyimpan dan menggunakan

perisian yang tidak berlesen dan segala bentuk perisian hiburan seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet. Pengguna juga dilarang menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

1.16 Pengguna hendaklah mematuhi tatacara dan peraturan yang telah ditetapkan agar keselamatan ke atas pemakaiannya akan terus terjamin. Peranan dan tanggungjawab pengguna adalah seperti berikut:

(a) Menggunakan akaun atau alamat e-mel yang diperuntukkan oleh jabatan;

(b) Memaklumkan kepada pentadbir sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

(c) Menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian, iaitu seperti berikut;

i. Rahsiakan kata laluan anda dari pengetahuan orang lain. Pendedahan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997.

ii. Sekiranya kata laluan telah dikompromi atau disyaki dikompromi, hendaklah dilaporkan kepada pentadbir sistem ICT dan kata laluan sedia ada diubah dengan serta merta.

iii. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian.

iv. Kata laluan hendaklah mempunyai saiz sekurang-kurangya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus.

v. Elakkan dari menggunakan semula kata laluan yang terdahulu.

vi. Kata laluan hendaklah dihafal dan TIDAK BOLEH dicatat, disimpan atau dideahkan dengan apa cara sekalipun.

(d) Memastikan setiap fail yang dimuat turun bebas dari virus sebelum digunakan;

(e) Bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik e-mel di dalam akaun sendiri. Dengan itu, pengguna perlu bertindak bijak, professional dan berhati-hati apabila berkomunikasi menerusi saluran elektronik;

(f) Berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman Internet yang

mengandungi unsur-unsur yang tidak menyenangkan, lucah atau negatif;

(g) Mengadakan salinan atau pendua pada media storan kedua elektronik seperti thumbdrive dan sebagainya bagi tujuan keselamatan;

(h) Memastikan kemudahan e-emel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-emel yang dialamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan;

(i) Menggunakan kemudahan password screen saver atau log keluar apabila hendak meninggalkan komputer;

(j) Memaklumkan kepada pentadbir sistem ICT sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan; dan

(k) Memaklumkan kepada pentadbir sistem ICT atau pegawai keselamatan ICT (ICTSO) sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan ICT.

1.17 Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) dengan kadar segera;

a) Maklumat didapati hilang, didedahkan kepada 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 laluan (password) hilang atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

1.18 Pihak UTM, PMK bertanggungjawab untuk melaporkan segala salah laku pelanggaran peraturan dan pekeliling kepada pihak pengurusan PMK dengan menyatakan nama / jabatan jika ada antara warga kerja PMK yang terlibat. Seluruh warga kerja PMK perlu merujuk kepada Dasar Keselamatan ICT dan Pekeliling/Surat Pekeliling/Arahan/Surat Arahan, serta Akta yang sedang berkuatkuasa dan berkaitan dengan penggunaan kemudahan ICT supaya tidak terlibat dalam pelanggaran mana-mana peraturan yang ditetapkan.

PENUTUP

Memelihara dan melindungi pelbagai aspek keselamatan jabatan adalah merupakan tanggungjawab setiap warga kerja PMK. Justeru bagi memastikan ia dilaksanakan secara menyeluruh, warga PMK hendaklah sentiasa menggunapakai SOP Keselamatan Umum Pejabat PMK yang disediakan ini bagi melancarkan pelaksanaan tugas rutin harian secara lebih selamat dan berterusan.

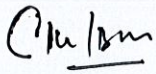
Tarikh Berkuatkuasa : 27 Mei 2019

Disediakan oleh :

Pegawai Keselamatan Jabatan
Politeknik Melaka

MOHD ARIFFIN BIN AMAN
Timbalan Pengarah
Politeknik Melaka

Diluluskan oleh :



Pengarah,
Politeknik Melaka

CHARIM BIN IBRAHIM@BERAHIM
Pengarah
Politeknik Melaka