GARIS PANDUAN

KESELAMATAN PERLINDUNGAN

POLITEKNIK BALIK PULAU

Politeknik Balik Pulau
Pulau Pinang
Oktober 2020

GARIS PANDUAN
KESELAMATAN PERLINDUNGAN
POLITEKNIK BALIK PULAU

Garis Panduan Keselamatan Perlindungan ini disediakan untuk memberi panduan serta kefahaman kepada semua warga Politeknik Balik Pulau berhubung keselamatan perlindungan dan seterusnya memastikan urusan keselamatan perlindungan di Politeknik Balik Pulau sentiasa diberi perhatian dan keutamaan serta menepati kehendak Arahan Keselamatan Kerajaan Malaysia.

Garis Panduan ini perlu dirujuk dan dibaca bersama:-

i. Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan, Jabatan Perdana Menteri.
ii. Garis Panduan Pelantikan Pegawai Pengelas Kementerian Pendidikan Malaysia, Mei 2019
iii. Arahan Pentadbiran Pengurusan Rekod Jabatan Perkhidmatan Awam Bilangan 1 2018
iv. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 : Panduan Pengurusan Pejabat
v. Polisi Keselamatan Siber KPM Versi 1.0 yang dikeluarkan oleh Kementerian Pendidikan Malaysia, April 2019
vi. Buku Panduan Keselamatan Pengurusan Teknologi Maklumat & Komunikasi Sektor Awam Malaysia (MyMIS), 2002.
vii. Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) (Pekeliling Am Bil. 1 Tahun 2001).
viii. Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan (Pekeliling Am Bil. 3 Tahun 2000).
ix. Dasar Keselamatan ICT Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), Versi 5.3

Kawalan keselamatan perlindungan di dalam garis panduan ini dibahagikan kepada lima (5) bahagian utama :-

1. Keselamatan Perlindungan
2. Keselamatan Fizikal
3. Keselamatan Dokumen
4. Keselamatan Peribadi
5. Keselamatan Penggunaan Teknologi Maklumat dan Komunikasi

ISI KANDUNGAN

Perkara	Muka surat

Perkara	Muka surat

SENARAI SINGKATAN

PBU	Politeknik Balik Pulau
PKJ	Pegawai Keselamatan Jabatan
PPKJ	Penolong Pegawai Keselamatan Jabatan
PKPKK	Pejabat Ketua Pegawai Keselamatan Kerajaan
TMK	Teknologi Maklumat & Komunikasi
UKP	Unit Khidmat Pengurusan
UICT	Unit Teknologi Maklumat dan Komunikasi

CDROM	*Compact Disc Read Only Memory*
CERT	*Computer Emergency Response Team*
ICT	*Information & Communication Technology*

TAFSIRAN ISTILAH

Aset	-	Meliputi perkara maklumat rasmi, dokumen rasmi dan rahsia rasmi, bangunan, pepasangan, peralatan, kelengkapan dan personel.
Dokumen Rasmi	-	Apa-apa jenis maklumat yang tercatat berkenaan dengan perkara rasmi.
Dokumen Terperingkat	-	Dokumen rasmi yang mengandungi maklumat rasmi yang diberi perlindungan untuk keselamatan dan bertanda dengan sesuatu peringkat keselamatan.
Maklumat Terperingkat	-	Maklumat rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan.
Perkara Rasmi	-	Termasuk segala dokumen rasmi, maklumat rasmi dan bahan rasmi.
Perkara Terperingkat	-	Perkara rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan.
Kawasan Terperingkat	-	Kawasan premis atau sebahagian daripada premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Buangan Terperingkat	-	Semua catatan, deraf, kertas karbon, stensil dan lain-lain bahan yang digunakan untuk menghasilkan perkara terperingkat yang tidak diperlukan lagi.
Meteri	-	Bahan *Sulit* yang dibekalkan kepada jabatan untuk memeterikan lakri di sampul surat yang mengandungi perkara terperingkat.
Anak Kunci Keselamatan	-	Anak kunci untuk membuka peti keselamatan atau bilik-bilik keselamatan.
Peti atau Beg Berkunci	-	Peti atau Beg yang digunakan untuk penghantaran dokumen terperingkat yang dilengkapkan dengan kunci keselamatan.

1.0 KESELAMATAN PERLINDUNGAN

1.1 Takrif dan Kepentingan Keselamatan Perlindungan

Keselamatan Perlindungan bermaksud memberi perlindungan ke atas aset yang meliputi perkara maklumat rasmi, dokumen rasmi dan rahsia rasmi, bangunan, pepasangan, peralatan, kelengkapan dan personel.

Pengurusan keselamatan perlindungan adalah pendekatan, sistem dan langkah-langkah yang diambil atau dilaksanakan bagi memasti keberkesanan pelaksanaan keselamatan perlindungan di sesebuah organisasi. Pengurusan keselamatan perlindungan yang sistematik dan teratur mengikut arahan serta panduan yang telah ditetapkan adalah sangat penting memandangkan keselamatan aset perlu dijaga supaya sentiasa selamat dan tidak jatuh ke tangan pihak yang ada kepentingan terutamanya kuasa-kuasa asing yang boleh mengancam keselamatan negara.

1.2 Ketua Jabatan

Pengarah sebagai Ketua Jabatan bertanggungjawab sepenuhnya mengenai hal keselamatan perlindungan di Politeknik Balik Pulau. Pengarah perlu mengambil langkah mengikut peruntukan–peruntukan Arahan Keselamatan bagi memastikan perkara terperingkat di Politeknik Balik Pulau dikawal dengan sempurna setiap masa. Pengarah juga bertanggungjawab mengemukakan laporan keselamatan kepada Pegawai Keselamatan Kerajaan apabila diminta berbuat demikian.

1.3 Pegawai Keselamatan Jabatan

Timbalan Pengarah Sokongan Akademik adalah pegawai yang dilantik sebagai Pegawai Keselamatan Jabatan (PKJ) dan bertanggungjawab melaksanakan arahan-arahan keselamatan Kerajaan di Politeknik Balik Pulau, dengan mendapat nasihat daripada Pegawai Keselamatan Kerajaan. Tugas Pegawai Keselamatan Jabatan ini adalah sebagai tugas tambahan kepada tugas-tugas hakiki beliau.

1.4 Buku Arahan Keselamatan

Buku Arahan Keselamatan mengandungi Arahan Keselamatan yang dikeluarkan oleh Jemaah Menteri mengenai peraturan-peraturan kawalan keselamatan perlindungan untuk Ketua-Ketua Jabatan di semua Kementerian, Jabatan, Badan Berkanun dan Agensi Kerajaan di peringkat Persekutuan dan Negeri.

Arahan Keselamatan yang terkandung di dalam buku ini menetapkan darjah-darjah keselamatan yang sama mengikut prinsip-prinsip tertentu untuk dilaksanakan di semua Jabatan dan Agensi Kerajaan. Setiap penjawat awam yang diamanahkan dengan perkara terperingkat dikehendaki mematuhi peruntukan-peruntukan yang terkandung di dalam Arahan Keselamatan tersebut dan dijadikan amalan biasa bagi pengurusan perkara-perkara rasmi yang perlu diberi perlindungan keselamatan.

Buku ini boleh diperolehi daripada Pejabat Ketua Pegawai Keselamatan Kerajaan dan perlu dikawal mengikut peraturan-peraturan keselamatan yang ditetapkan Ketua Pengarah Keselamatan Kerajaan.

1.5 Arahan Keselamatan Jabatan

Arahan Keselamatan Jabatan adalah arahan-arahan yang dikeluarkan oleh Pengarah selaku Ketua Jabatan atau Timbalan Pengarah Sokongan Akademik selaku Pegawai Keselamatan Jabatan dari masa ke semasa berkaitan dengan keselamatan perlindungan di Politeknik Balik Pulau. Arahan-arahan ini perlu dipatuhi dan dilaksanakan oleh semua warga Politeknik Balik Pulau.

Garis Panduan Keselamatan Politeknik Balik Pulau ini merupakan satu contoh Arahan Keselamatan Jabatan.

1.6 Kursus Keselamatan Perlindungan

Pengawai Keselamatan Jabatan perlu memastikan semua warga PBU diberi pendedahan kepada aspek-aspek keselamatan perlindungan secara umum dan juga secara khusus bagi warga PBU yang terlibat dengan perkara-perkara khusus yang memerlukan perlindungan keselamatan.

Pengawai Keselamatan Jabatan perlu merancang program-program yang bersesuaian bagi memastikan semua warga PBU diberi pengetahuan dan kemahiran dalam hal berkaitan keselamatan perlindungan agar semua warga PBU sedar dan faham kepentingan keselamatan perlindungan.

Pegawai Keselamatan Jabatan juga perlu mengenal pasti dan menggunakan pelbagai kaedah dan pendekatan bagi memastikan kesedaran semua warga PBU ditahap yang baik dan tiada seorang warga PBU boleh memberi alasan tidak tahu berkaitan keselamatan perlindungan.

1.7 Pelanggaran Keselamatan

Pelanggaran keselamatan berlaku apabila ada kejadian atau insiden yang menyebabkan keselamatan aset yang meliputi perkara maklumat rasmi, dokumen rasmi dan rahsia rasmi, bangunan, pepasangan, peralatan, kelengkapan dan personel diancam atau dikompromi.

Sebarang pelanggaran keselamatan adalah dianggap serius dan tidak boleh dikompromi.

Warga PBU yang mengetahui, mengesan atau mengesyaki kejadian atau perbuatan pelanggaran keselamatan dikehendaki melaporkannya dengan serta merta kepada Pegawai Keselamatan Jabatan atau Pengarah. Sebarang pelanggaran keselamatan akan disiasat dan tindakan tegas akan diambil mengikut peruntukan undang-undang dan peraturan yang berkaitan yang sedang berkuatkuasa.

Pendakwaan di bawah Akta Rahsia Rasmi 1972 atau tindakan tatatertib boleh diambil terhadap mana-mana warga PBU yang cuai, lalai atau terlibat dalam pelanggaran keselamatan.

2.0 KESELAMATAN FIZIKAL

Keselamatan fizikal merujuk kepada perancangan dan tindakan yang dilaksanakan bagi memastikan keselamatan kawasan, infrastruktur dan kemudahan fizikal Politeknik Balik Pulau diberi perlindungan yang sewajarnya mengikut peraturan dan arahan keselamatan.

Pengarah dan PKJ bertanggungjawab mengkaji keperluan keselamatan fizikal dan memastikan perlindungan keselamatan diberi sepenuhnya terutama bagi kawasan-kawasan yang sensitif dan perlu diberi perlindungan tertentu.

2.1 Keselamatan Kawasan

Keselamatan kawasan Politeknik Balik Pulau perlu dberi perhatian yang serius bagi memastikan tidak berlaku sebarang bentuk pencerobohan.

Antara langkah-langkah yang perlu diambil dan diberi penekanan adalah :-

2.1.1 Memastikan keseluruhan pagar premis PBU dan pintu-pintu pagar sentiasa berada dalam keadaan baik serta selamat.

2.1.2 Memastikan lampu-lampu keselamatan diadakan dan berfungsi dengan baik serta menepati keperluan pencahayaan keselamatan.

2.1.3 Mengadakan kawalan keselamatan dengan kuasa-kuasa tertentu dan dilengkapi peralatan keselamatan di pintu masuk dan lain-lain tempat yang dikenalpasti keperluannya.

2.1.4 Mengadakan papan tanda keselamatan di tempat-tempat yang sesuai.

2.1.5 Mewujudkan sistem pengenalan diri atau pas keselamatan yang sesuai.

2.1.6 Memastikan peralatan tv litar tertutup (CCTV) sentiasa berfungsi dengan baik.

2.1.7 Memastikan kebersihan keseluruhan premis PBU, kawasan dan bangunan, sentiasa melebihi tahap baik.

2.2 Keselamatan Bangunan

Langkah-langkah keselamatan terhadap semua bangunan adalah bertujuan menghalang orang-orang yang tidak dibenarkan daripada menceroboh atau mendapat akses kepada aset PBU samada dari dalam atau luar premis PBU secara haram.

Antara langkah-langkah yang perlu diambil dan diberi penekanan oleh Pegawai Keselamatan Jabatan adalah :-

2.2.1 Sistem Pengenalan Diri atau Pas Keselamatan

a. Pas Keselamatan dikeluarkan kepada semua individu yang memasuki atau berada di dalam kawasan PBU berdasarkan kategori berikut :

   i. Pas Keselamatan Tetap (dikeluarkan kepada semua staf PBU)

   ii. Pas Keselamatan Pelawat (dikeluarkan kepada pelawat)

   iii. Pas Keselamatan Pekerja Kontrak

   iv. Pas Keselamatan Pelajar

b. Semua staf perlu membawa dan menunjukkan Pas Keselamatan masing-masing apabila diminta oleh pihak kawalan keselamatan.

c. Semua pelawat dan pekerja kontrak perlu memakai/mempamirkan Pas Keselamatan masing-masing dan memulangkannya kepada pihak kawalan keselamatan apabila meninggalkan premis PBU.

d. Kehilangan Pas Keselamatan perlu dilaporkan kepada pihak yang mengeluarkan Pas Keselamatan tersebut.

2.2.2 Buku Daftar Pelawat dan Borang Pelawat

a. Setiap pelawat yang memasuki premis perlu mendaftar di Balai Pengawal di pintu masuk PBU dan mendapatkan Pas Keselamatan serta Borang Pelawat.

b. Setiap pelawat perlu mendapatkan pengesahan pegawai PBU yang ditemui dan mengembalikan Borang Pelawat dan Pas Keselamatan kepada pihak Pengawal Keselamatan di Balai Pengawal sebelum meninggalkan premis PBU.

2.2.3 Kaunter Pelanggan atau Pelawat

a. Kaunter Pelanggan atau Pelawat disediakan bagi tujuan membantu pelanggan atau pelawat mendapat perkhidmatan, maklumat atau panduan disamping menghadkan pergerakan pelanggan atau pelawat.

b. Pihak Unit Khidmat Pengurusan (UKP) perlu memastikan ada petugas yang bertugas di kaunter di sepanjang waktu pejabat.

c. Lampu di ruang legar Kaunter Pelanggan atau Pelawat perlu dipasang sepanjang malam.

2.2.4 Sistem Staf Bertugas Harian

a. Setiap jabatan/pusat/unit di PBU yang mempunyai ruang pejabat, bilik atau kemudahan sendiri perlu mengadakan sistem staf bertugas harian bagi mengawal dan memantau keselamatan jabatan, pusat dan unit masing-masing.

b. Ketua jabatan/pusat/unit bertanggungjawab melantik dan menyediakan jadual staf bertugas berserta senarai tugas dan tanggungjawab yang perlu dilaksanakan.

c. Jadual staf bertugas perlu dipamer di lokasi yang sesuai sebagai peringatan kepada staf yang bertugas dan juga sebagai panduan dan rujukan umum.

d. Ketua jabatan/pusat/unit bertanggungjawab menyediakan borang laporan staf bertugas harian dan borang ini hendaklah diisi oleh staf yang bertugas setiap hari dan diserahkan kepada ketua jabatan/pusat/unit untuk tindakan selanjutnya.

e. Laporan harian staf bertugas harian akan dijadikan sebagai rujukan sekiranya berlaku sebarang insiden pelanggaran keselamatan perlindungan di jabatan/pusat/unit berkenanan.

f. Ketua jabatan/pusat/unit bertanggungjawab melaporkan status pelaksanaan staf bertugas kepada Pegawai Keselamatan Jabatan apabila diminta berbuat demikian.

g. Pegawai Keselamatan Jabatan bertanggungjawab memantau pelaksanaan sistem staf bertugas secara berkala atau secara mengejut bagi memastikan pelaksanaan sistem staf bertugas dilaksanakan dengan sempurna.

h. Sistem staf bertugas harian ini hendaklah dilaksanakan setiap hari bekerja dan secara “on call” pada hari-hari cuti mingguan dan cuti umum.

2.2.5 Keselamatan Pintu dan Tingkap Bangunan, Sistem Penggera dan Siaraya

a. Pintu dan tingkap perlu dilengkapkan dengan kunci keselamatan yang bersesuaian.

b. Pintu dan tingkap bangunan perlu diperkukuhkan dengan cara yang bersesuaian sekiranya perlu.

c. Pintu dan tingkap hendaklah sentiasa dipastikan dikunci dengan selamat terutamanya sebelum meninggalkan pejabat atau bangunan.

d. Sistem penggera keselamatan kebakaran di PBU perlu diselenggara dan dipastikan berfungsi dengan baik.

e. Sistem siaraya yang bertujuan untuk memberi hebahan maklumat kepada warga PBU perlu dipastikan berfungsi dengan baik.

2.2.6 Pengurusan Kunci Keselamatan

a. Mewujud dan menyelenggara Buku Daftar Kunci serta memeriksa buku tersebut secara berkala.

b. Memastikan pemegang anak kunci dimaklumkan tentang tanggungjawab dan risiko yang hadapi apabila memegang dan menyimpan kunci.

c. Memastikan pengurusan kunci dibuat mengikut prosedur atau tatacara mengurus kunci yang ditetapkan.

d. Memastikan anak kunci serta kunci-kunci pendua dilabel menggunakan kod-kod tertentu dan tidak dilabel atau ditanda dengan nama lokasi.

e. Memastikan anak kunci termasuk kunci pendua disimpan dengan selamat mengikut prosedur atau tatacara penyimpanan kunci.

f. Mewujudkan Buku Pergerakan Kunci bagi memudahkan pengesanan pergerakan anak kunci.

g. Memastikan setiap warga yang berpindah atau berhenti daripada perkhidmatan kerajaan menyerahkan semua anak kunci kepada pegawai yang bertanggungjawab.

h. Melaporkan dengan segera sebarang kehilangan anak kunci kepada Pegawai Keselamatan Jabatan atau Pengarah. Laporan kehilangan hendaklah dikemukakan kepada Pegawai Keselamatan Kerajaan dalam tempoh 24 jam dari waktu kehilangan kenalpasti.

2.3 Perkhidmatan Kawalan Keselamatan

Kawalan keselamatan di Politeknik Balik Pulau adalah dikendalikan oleh syarikat luar secara kontrak. Tugas kawalan keselamatan diperincikan dalam dokumen kontrak kawalan keselamatan.

Secara umumnya perkara-perkara berikut adalah di bawah bidang tugas dan tanggungjawab Pengawal Keselamatan :-

a. Mengawal dan memantau keluar masuk staf, pelajar, pelawat dan orang awam yang memasuki premis Politeknik Balik Pulau. Kawalan keselamatan ini antara lain termasuk merekod maklumat dalam buku daftar, pengeluaran pas dan borang pelawat.

b. Mengiringi kontraktor, pelawat atau orang awam yang ada urusan di politeknik ke kaunter pelanggan atau pelawat untuk urusan bertemu dengan staf politeknik berkenaan.

c. Mengawal dan memantau pergerakan staf, pelajar, pelawat dan orang awam yang berada di dalam politeknik.

d. Meminta dan memastikan pelawat memakai pas keselamatan yang dibekalkan.

e. Membuat pemeriksaan secara rawak ke atas kenderaan yang keluar masuk kawasan politeknik bagi memastikan keselamatan aset politeknik sentiasa terpelihara.

f. Memastikan setiap kenderaan warga politeknik dan pelajar mempunyai pelekat pendaftaran yang sah dan dipamirkan.

g. Memastikan hanya mereka yang ada atau mendapat kebenaran sahaja dibenarkan masuk dan berada di dalam kawasan Politeknik Balik Pulau.

h. Mengawal dan memantau kenderaan yang keluar masuk kawasan Politeknik.

i. Memastikan semua kenderaan diparkir di tempat yang ditetapkan.

j. Mengawal lalu-lintas di hadapan pintu utama politeknik dan keseluruhan kawasan politeknik.

k. Menghalang jurujual atau *promoter* produk atau perkhidmatan yang tidak mempunyai surat kebenaran pihak politeknik daripada memasuki kawasan politeknik.

l. Menghubungi pihak-pihak berkuasa dan agensi seperti Jabatan Bomba dan Penyelamat, Polis Diraja Malaysia, Angkatan Pertahanan Awam Malaysia dan Hospital sekiranya berlaku apa-apa insiden kecemasan atau insiden yang mengancam keselamatan Politeknik Balik Pulau.

2.4 Kawalan Peralatan Penyalin

a. Setiap mesin penyalin perlu diletakkan di lokasi yang sesuai dan selamat.

b. Seorang staf perlu dilantik berserta dengan senarai tugas untuk menjaga dan mengawal penggunaan mesin penyalin yang disediakan dimana-mana lokasi yang dikenalpasti.

c. Setiap mesin penyalin perlu disediakan buku rekod penggunaan dan buku rekod ini perlu diisi oleh pengguna mesin penyalin berkenaan dan perlu diselenggara dan diperiksa secara berkala oleh pegawai yang bertanggungjawab terhadap mesin tersebut.

d. Semua salinan dokumen yang rosak atau yang tidak diperlukan hendaklah dirincih atau musnahkan.

e. Bagi dokumen terperingkat, hanya staf yang dibenarkan sahaja yang boleh ditugaskan untuk membuat salinan dokumen terperingkat mengikut prosedur menyalin dokumen terperingkat.

f. Setiap perlakuan salahguna mesin penyalin hendaklah dilaporkan kepada pegawai penyelia atau ketua jabatan dan tindakan tatatertib hendaklah diambil mengikut peraturan yang sedang berkuat kuasa.

g. Pegawai yang bertanggungjawab terhadap mana-mana mesin penyalin hendaklah memastikan maklumat atau data yang tersimpan di dalam ingatan atau *memory* mesin penyalin dipadam sepenuhnya secara berkala dan sebelum mesin dikembalikan pihak pembekal mesin penyalin sekiranya mesin tersebut disewa.

2.5 Kawalan Peti Besi dan Bilik Kebal

a. Memastikan peti besi dan bilik kebal sentiasa diurus, dikawal dan diselenggara mengikut prosedur keselamatan peti besi dan bilik kebal.

b. Buku Daftar Kunci Keselamatan dan Buku Daftar Pergerakan hendaklah diwujudkan, dikawal, diselenggara dan diperiksa mengikut prosedur berkaitan.

c. Kawalan peti besi dan bilik kebal hendaklah dilaksanakan oleh dua (2) orang staf daripada Kumpulan Pengurusan & Profesional atau Kumpulan Sokongan I. Seorang staf akan bertanggungjawab terhadap nombor kombinasi kunci dan seorang lagi bertanggungjawab terhadap anak kunci peti besi dan bilik kebal.

d. Staf yang diberi tanggungjawab memegang dan menjaga nombor kombinasi atau anak kunci keselamatan peti besi atau bilik kebal hendaklah dilantik secara rasmi untuk memastikan tanggungjawab keselamatan nombor kombinasi dan anak kunci dijaga.

e. Nombor kombinasi perlu ditukar sekurang-kurangnya sekali setiap tahun atau apabila berlaku pertukaran staf yang bertanggungjawab atau disyaki nombor kombinasi telah dikompromi.

f. Nombor kombinasi hendaklah diurus/disimpan mengikut prosedur “Rahsia Besar”.

g. Pintu peti besi atau bilik kebal hendaklah dikunci setiap kali selepas akses.

h. Staf yang bertanggungjawab hendaklah menyerah anak kunci keselamatan kepada PKJ atau ketua jabatan apabila bertukar atau berhenti atau meninggalkan perkhidmatan.

i. Perincian berkaitan peti keselamatan, bilik kebal dan kunci keselamatan adalah seperti di Lampiran F Arahan Keselamatan.

2.6 Kelengkapan dan Bahan-Bahan Rasmi Dengan Ciri Keselamatan

a. Sebarang cadangan perolehan dan penggunaan kelengkapan dan bahan-bahan rasmi yang mempunyai ciri-ciri keselamatan di PBU perlu dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan.

b. Kelenggkapan dan bahan-bahan yang mempunyai ciri-ciri keselamatan yang dinyatakan di perkara 2.6 a. di atas meliputi :-

   i. Kelengkapan dan bahan-bahan teknik, mekanik, elektrik dan elektronik termasuk kunci keselamatan, pagar dan lampu keselamatan, perakam kad akses, penggera keselamatan, televisyen litar tertutup, peti keselamatan, pengalisan bunyi, alat anti pengesan suara, komputer, mesin saifer, mesin cetak, mesin penyalin, mesin perincih, *incinerator* dan lain-lain perkakas, bahan atau kelengkapan yang digunakan dalam keselamatan perlindungan.

ii. Kelengkapan dan bahan-bahan yang jenis bukan teknik, mekanik, elektrik dan elektronik termasuk mata wang, kad pengenalan, pasport dan dokumen perjalanan, setem, lesen, kertas peperiksaan, kertas-kertas keselamatan, sijil – termasuk sijil kerakyatan, skrol ijazah, watikah-watikah darjah kebesaran, mikrofilem, pita komputer, buku akaun bank, permit, perintah kiriman wang pos, borang-borang dan dokumen hasil, peta, mohor, meteri dan lain-lain perkakas, bahan atau kelengkapan yang digunakan dalam keselamatan perlindungan.

3.0 KESELAMATAN DOKUMEN

Keselamatan dokumen bermaksud tindakan-tindakan yang dilaksanakan terhadap dokumen terperingkat di PBU untuk memastikan dokumen selamat daripada pendedahan kepada atau diakses oleh mereka yang tidak dibenarkan.

3.1 Dokumen Rasmi

a. Dokumen rasmi adalah apa-apa jenis maklumat yang tercatat berkenaan dengan perkara-perkara rasmi dan ini merangkumi :

   i. Perkara yang bertulis, bertaip, bertulis trengkas, disalin, berstensil, bercetak dan juga deraf dan buangan dari perkara itu;

   ii. Fotograf, foto salinan, pelan cetak, negatif foto dan filem, jalur suara dan rakaman;

   iii. Pelan, pelan lakar, lukisan, gambarajah, peta dan pelbagai jenis carta;

   iv. Huruf cetak atur atau huruf cetak miring, blok litografer, acuan, stensil, proses plat atau lain-lain alat yang digunakan untuk membuat dokumen rasmi.

b. Dokumen rasmi terbahagi kepada dua (2) iaitu dokumen terperingkat dan dokumen tidak terperingkat. Dokumen terperingkat mengandungi maklumat rasmi yang terperingkat dan ditanda dengan peringkat keselamatannya manakala dokumen tidak terperingkat mengandungi maklumat rasmi tetapi tidak diberi tanda peringkat keselamatan.

3.2 Pengurusan Dokumen Terperingkat

3.2.1 Dokumen Terperingkat

a. Dokumen terperingkat adalah dokumen rasmi yang mengandungi maklumat rasmi yang diberi perlindungan untuk kepentingan keselamatan dan yang bertanda dengan sesuatu peringkat keselamatan samada *Rahsia Besar*, *Rahsia*, *Sulit* atau *Terhad*.

b. Pengurusan dokumen terperingkat merangkumi peringkat penyediaan, penyimpanan, pengesahan, penghantaran dan pemusnahan. Pengurusan ini perlu mengikut arahan, pekeliling atau peraturan keselamatan yang ditetapkan.

c. Hanya staf atau pegawai yang diberi kebenaran sahaja boleh mengurus atau mengendalikan dokumen terperingkat.

3.2.2 Peringkat Keselamatan

a. Perkara terperingkat perlu diperingkatkan mengikut peringkat keselamatan seperti berikut :-

   i. ***Rahsia Besar*** – Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada nagara.

   ii. ***Rahsia*** – dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa *kebenaran* akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat negara atau memberi keuntungan besar kepada sesebuah kuasa asing.

iii. ***Sulit*** – dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat negara atau kegiatan kerajaan atau orang *perseorangan* atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.

iv. ***Terhad*** – dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan *sebagai* Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.

b. Staf yang diberi kebenaran untuk mengendalikan dokumen terperingkat perlu merujuk kepada perkara 45 Arahan Keselamatan berhubung peraturan-peraturan bagi memperingkatkan dokumen dengan peringkat keselamatan yang betul.

c. Penyedia atau pemula sesuatu perkara terperingkat bertanggungjawab membuat ulangkaji terhadap peringkat keselamatan perkara tersebut. Ini bertujuan mengubah peringkat keselamatan sesuatu perkara jika perlu dan sekiranya berlaku perubahan peringkat keselamatan, pemakluman perubahan peringkat perlu dimaklumkan kepada mereka yang berkenaan. Perkara terperingkat yang dimaksudkan akan menjadi kurang penting keselamatannya pada sesuatu tarikh yang ditetapkan hendaklah ditulis demikian oleh penyedia atau pemulanya dengan menyatakan tarikh dan peringkat yang baharu atau bahawa perkara itu akan menjadi tiada terperingkat.

3.2.3 Pegawai Pengelas

a. Pegawai Pengelas adalah seorang pegawai awam yang dilantik mengikut Seksyen 2B Akta Rahsia Rasmi 1972 bertujuan untuk mengelaskan surat rasmi, maklumat dan bahan sebagai *Rahsia Besar, Rahsia, Sulit* atau *Terhad* mengikut mana yang berkenaan.

b. Pelantikan Pegawai Pengelas adalah merujuk kepada Surat Pekeliling Am Bil. 2 Tahun 1987 bertarikh 20 Februari 1987.

c. Pegawai Pengelas adalah berperanan untuk membuat pengelasan maklumat berdasarkan proses berikut :-

i. Menyemak

- Menentukan dokumen yang dibuat semakan adalah dokumen PBU.

ii. Menilai

- Menilai taraf keselamatan dokumen samada *Rahsia Besar, Rahsia, Sulit* atau *Terhad* mengikut tafsiran Arahan Keselamatan seperti di perkara 3.2.2 a. di atas.

iii. Memberi Tanda

- Dokumen diberi tanda pengelasan mengikut peringkat keselamatan yang ditetapkan di setiap mukasurat dokumen dan

iv. Mendaftar

- Merekod dalam Buku Daftar Suratan Rahsia Rasmi di Luar Jadual / bawah Jadual Akta Rahsia Rasmi 1972 dan ditandatangani oleh Pegawai Pengelas.

d. Pegawai Pengelas juga bertanggungjawab memastikan tindakan-tindakan berikut dilaksanakan seperti mana yang dinyatakan dalam Seksyen 2B Akta Rahsia Rasmi :-

i. Memastikan pelaksanaan pendaftaran suratan rasmi yang dikelaskan dan dikelaskan semula dalam Buku Daftar Suratan Rahsia Rasmi iaitu Am 492, Am 492A dan Am 492B mengikut mana yang berkenaan;

ii. Kesemua buku daftar ini perlu dikawal dan disimpan dengan selamat dan perlu ditender dalam mahkamah sebagai bahan bukti mengenai pengelasan semula rahsia rasmi yang ditetapkan;

iii. Memaklumkan semua pihak terlibat mengikut suratan asal tersebut untuk memaklumkan bahawa suratan tersebut telah dikelaskan semula atau terhenti menjadi rahsia rasmi dan

iv. Memaklumkan kepada urus setia BKP bagi urusan penyelarasan pengelasan semula atau penurunan taraf peringkat atau pelupusan sewajarnya dengan Jabatan Arkib Negara Malaysia dan Pejabat Ketua Pegawai Keselamatan Kerajaan.

3.2.4 Pendaftar Rahsia

Pendaftar Rahsia adalah seorang pegawai yang dilantik bagi mengurus dokumen terperingkat. Antara tugas dan tanggungjawab Pendaftar Rahsia adalah :

a. Melaksanakan tugas dan tanggungjawab Pendaftar Rahsia mengikut arahan dan peraturan keselamatan yang ditetapkan.

b. Menyimpan rekod dokumen terperingkat yang peringkatnya tidak rendah daripada Sulit.

c. Menerima dan memproses dokumen terperingkat serta mengedarkannya kepada pegawai yang berkenaan mengikut arahan jabatan.

d. Menghantar dokumen terperingkat dengan selamat dan menentukan akuan terima bagi dokumen terperingkat yang dihantar.

e. Menyelenggara sistem pegerakan dokumen terperingkat dan rekod pergerakan dokumen terperingkat.

f. Bertanggungjawab sepenuhnya kepada Pengarah berkaitan keselamatan pendaftaran rahsia termasuk penyimpanan semua perkara teperingkat.

3.3 Tanda Keselamatan

Dokumen terperingkat perlu ditanda mengikut peringkat keselamatan yang ditetapkan.

3.3.1 Dokumen Terperingkat Yang Kekal dan Teguh Terjilid

Peringkat keselamatan hendaklah ditanda dengan huruf cerai atau dicap huruf besar (tidak kurang daripada 7mm) di sebelah luar kulit hadapan dan belakang, di mukasurat tajuk, di mukasurat pertama dan penghabisan. Peringkat keselamatan hendaklah juga ditanda dengan huruf cerai atau dicap dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah di setiap mukasurat yang mengandungi perkara bertulis, bercetak atau bercap.

3.3.2 Dokumen Terperingkat Yang Tidak Kekal Atau Tidak Teguh Terjilid

Peringkat keselamatan hendaklah ditanda dengan dicap, ditaip atau ditulis dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah tiap-tiap mukasurat yang mengandungi perkara bertulis, bercetak atau bercap.

3.3.3 Lukisan, Tekapan, Negatif Foto Dan Gambar Foto Terperingkat

Peringkat keselamatan hendaklah ditanda supaya peringkat keselamatannya dapat dilihat pada salinan yang dibuat daripadanya. Sebagai tambahan, peringkat keselamatan hendaklah juga ditanda pada sebelah belakang gambar-gambar foto terperingkat.

3.3.4 Fail Terperingkat

i. Peringkat keselamatan hendaklah ditanda di sebelah luar kulit hadapan dan belakang. Nombor rujukan fail hendaklah ditulis di sebelah luar kulit hadapan dan tajuknya dicatatkan di sebelah dalam kulit hadapan. Hanya tajuk fail *Terhad* sahaja boleh dicatat di sebelah luar kulit hadapan.

ii. Kulit fail terperingkat adalah diberi warna tertentu;-

- kulit fail *Rahsia Besar* berwarna kuning dengan berpalang merah di sebelah luar kulit hadapan dan belakang;
- kulit fail *Rahsia* berwarna merah jambu dengan berpalang merah di sebelah luar kulit hadapan dan belakang;
- kulit fail *Sulit* berwarna hijau dan
- kulit fail *Terhad* berwarna putih.

3.3.5 Nombor Rujukan dan Nombor Mukasurat

Setiap dokumen terperingkat hendaklah diberi nombor rujukan. Nombor mukasurat hendaklah juga diberi kepada setiap muka dokumen terperingkat yang mengandungi lebih daripada satu mukasurat. Nombor mukasurat hendaklah dicatat di bahagian tengah sebelah atas setiap mukasurat dan nombor mukasurat berikutnya dicatat di penjuru kanan sebelah bawah setiap mukasurat.

3.4 Penyimpanan Perkara Terperingkat

Perkara terperingkat pula disimpan menggunakan kaedah penyimpanan yang sesuai dengan peringkatnya. Berikut adalah kaedah penyimpanan perkara terperingkat :-

a. Peringkat *Rahsia Besar* dan *Rahsia*

Dokumen hendaklah disimpan di dalam bilik kebal atau peti besi yang seelok-eloknya dengan kunci tatakira. Dokumen yang dalam tindakan boleh disimpan untuk sementara waktu dalam kabinet fail yang dikunci atau almari keluli yang dipasang dengan palang besi berkunci. Jika bangunan yang dididuduki tidak mempunyai kawalan keselamatan yang rapi, dokumen tersebut hendaklah dikembalikan untuk simpanan di dalam bilik kebal atau besi.

b. Peringkat *Sulit* dan *Terhad*

Dokumen hendaklah disimpan di dalam kabinet keluli atau almari keluli berkunci.

c. Perkara terperingkat selain dokumen terperingkat termasuk buangan terperingkat yang belum dibinasakan hendaklah disimpan mengikut perkara 3.4 a. dan 3.4 b. di atas, kecuali sekiranya keadaan tidak membenarkan maka hendaklah disimpan mengikut peraturan yang dibenarkan oleh Pegawai Keselamatan Jabatan dengan persetujuan Pegawai Keselamatan Kerajaan.

d. Semua perkara terperingkat tidak boleh ditinggalkan tanpa perhatian. Sekiranya pegawai perlu meninggalkan ruang kerjanya, maka semua perkara terperingkat perlu disimpan di dalam kabinet atau almari keluli yang dikunci bagi mengelak daripada perkara terperingkat diakses atau dicapai oleh individu yang tidak dibenarkan.

e. Semua kunci bilik atau kabinet atau almari penyimpanan perkara terperingkat hendaklah disimpan di dalam peti keselamatan.

f. Ketua Jabatan/Pusat/Unit hendaklah memastikan pegawai yang bertukar atau meninggalkan perkhidmatan menyerahkan perkara terperingkat dan kunci berkaitan kepada Ketua Jabatan/Pusat/Unit atau pegawai yang mengambil alih tugas sebelum bertukar atau meninggalkan perkhidmatan.

3.5 Penghantaran Dokumen Terperingkat

a. Penghantaran semua dokumen terperingkat hendaklah menggunakan Borang Jadual seperti di Lampiran G Arahan Keselamatan. Borang Jadual perlu diisi dalam dua (2) salinan: salinan asal dihantar bersama dokumen terperingkat sementara satu salinan disimpan untuk rujukan. Resit akuan yang terima kembali hendaklah dilekatkan pada salinan simpanan.

b. Salinan Borang Jadual hendaklah disemak untuk memastikan resit akuan diterima daripada penerima dokumen terperingkat. Sekiranya resit akuan tidak diterima dalam tempoh tujuh (7) hari, surat peringatan hendaklah dihantar berserta siasatan serentak dijalankan untuk mengetahui kedudukan dokumen terperingkat yang dihantar. Sekiranya dokumen terperingkat yang dihantar tidak diterima dan tiada penjelasan yang memuaskan daripada pejabat yang menghantar dan yang dialamatkan, maka PKJ kedua–dua jabatan perlu dimaklumkan dengan segera. Jika resit akuan didapati hilang, pihak penerima dokumen perlu menghantar satu surat akuan penerimaan sebagai ganti kepada resit akuan tersebut.

c. Dokumen terperingkat yang dihantar melalui *Peti* atau *Beg Berkunci* dikehendaki menggunakan satu sampul surat sahaja. Sampul tersebut hendaklah ditanda dengan peringkat keselamatan dan nombor rujukan dokumen berkenaan serta nama dan alamat penerima dan dimeterikan dengan meteri pejabat yang menghantar.

d. Dikumen terperingkat yang dihantar tidak melalui *Peti* atau *Beg Berkunci* dikehendaki menggunakan dua (2) lapis sampul surat. Dokumen terperingkat dimasukkan ke dalam satu sampul surat dan hendaklah ditanda dengan peringkat keselamatan dan nombor rujukan dokumen berkenaan berserta nama dan alamat penerima dan dimeterikan dengan meteri pejabat yang menghantar. Sampul berisi dokumen terperingkat tersebut kemudian hendaklah dimasukkan ke dalam satu sampul lain yang bertulis nama dan alamat penerimanya sahaja dan ditutup dengan gam.

e. Perkara 65 Arahan Keselamatan hendaklah dirujuk bagi mengetahui prosedur penghantaran dokumen terperingkat mengikut peringkat keselamatan dan keadaan.

f. Penghantaran maklumat terperingkat melalui telefon atau faksimili atau emel adalah tidak dibenarkan. Sekiranya ada keperluan untuk berbuat demikian, permohonan perlu dibuat kepada Pegawai Keselamatan Kerajaan.

3.6 Membawa Dokumen Terperingkat Keluar Pejabat

a. Dokumen terperingkat tidak sekali-kali boleh dibawa keluar dari pejabat melainkan jika dikehendaki untuk rujukan rasmi di lain-lain tempat, dengan kebenaran bertulis Ketua Jabatan.

b. Dokumen terperingkat *Rahsia Besar* atau *Rahsia* tidak sekali-kali boleh dibawa balik ke rumah melainkan dengan kebenaran bertulis Ketua Setiausaha Kementerian atau Setiausaha Kerajaan Negeri berkenaan.

c. Bagi dokumen terperingkat *Sulit* atau *Terhad* pula, kebenaran Ketua Jabatan hendaklah diperolehi terlebih dahulu sebelum di bawa pulang ke rumah.

3.7 Pelepasan Perkara Terperingkat

a. Perkara terperingkat sama sekali tidak boleh dilepaskan kepada sesiapapun selain daripada yang dibenarkan tanpa kebenaran Ketua Jabatan.

b. Perkara terperingkat selain yang dimaksudkan untuk siaran segera kepada orang ramai dibawah syarat-syarat yang ditetapkan tidak sekali-kali boleh disampaikan kepada akhbar. Warga PBU salam sekali tidak dibenarkan menyampaikan maklumat terperingkat kepada pihak akhbar atau sesiapapun tanpa kebenaran Ketua Jabatan.

3.8 Pemusnahan Dokumen Terperingkat

a. Dokumen terperingkat sama sekali tidak boleh dimusnahkan melainkan mengikut arahan-arahan kerajaan kecuali jika terdapat arahan-arahan khas didokumen tersebut seperti "*Musnahkan Selepas 1hb April 1985*" atau "*Minta Kebenaran Pemula Sebelum Dimusnahkan*". Catatan di dalam daftar yang berkenaan perlu dibuat apabila sesuatu dokumen terperingkat dimusnahkan.

b. Apabila dokumen terperingkat Rahsia Besar dimusnahkan, satu sijil pemusnahan hendaklah dihantar kepada kuasa pemula dokumen tersebut. Pegawai Keselamatan Kerajaan hendaklah dirujuk sekiranya berkalu keadaan seperti kuasa pemula sudah tidak wujud lagi.

c. Ketua Pegawai Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara hendaklah dirujuk terlebih dahulu bagi cadangan pemusnahan dokumen terperingkat yang banyak yang difikirkan tidak lagi berguna untuk rujukan.

d. Dokumen terperingkat termasuk buangan terperingkat yang hendak dimusnahkan hendaklah terlebih dahulu dikoyak kecil-kecil atau dirincih dengan menggunakan mesin perincih dan dibakar mengikut peraturan-peraturan yang selamat di bawah penyeliaan penjawat awam yang dibenarkan mengendalikan dokumen tersebut. Abunya hendaklah dihancurkan sehingga tidak dikenali.

e. Buangan terperingkat hendaklah diberi perlindungan keselamatan sepatutnya sehingga dimusnahkan.

3.9 Kehilangan Dokumen Terperingkat

a. Dokumen terperingkat yang dipercayai hilang hendaklah dicari dengan segera dan kehilangan dilaporkan kepada Pegawai Keselamatan Jabatan atau Ketua Jabatan. Laporan siasatan yang mengandungi pandangan dan taksiran bahaya terhadap keselamatan hendaklah dikemukakan kepada Pegawai Keselamatan Kerajaan dalam tempoh 24 jam. Sekiranya kehilangan disahkan, pemula dokumen tersebut hendaklah dimaklumkan supaya taksiran risiko terhadap keselamatan dapat dibuat dan tindakan menyelamat dan pembetulan keadaan dapat diambil segera.

b. Jika dokumen terperingkat dibuktikan hilang, Ketua Jabatan hendaklah menimbang sama ada tindakan tatatertib wajar diambil atau penyiasatan di bawah Akta Rahsia Rasmi 1972 patut dijalankan. Laporan Polis hendaklah dibuat sekiranya difikirkan suatu kesalahan jenayah telah berlaku.

4.0 KESELAMATAN PERIBADI

4.1 Undang-Undang Berkaitan Perlindungan Rahsia Rasmi

a. Akta Rahsia Rasmi 1972 adalah satu akta undang-undang berhubung dengan perlindungan rahsia rasmi, terutama sekali dimaksudkan untuk memelihara perkara-perkara rasmi daripada jatuh ke tangan orang-orang yang tidak dibenarkan. Akta ini bertujuan untuk mencegah kelalaian yang bersalahan dan juga untuk menghalang apa-apa bantuan haram yang sengaja diberikan kepada agensi-agensi negara asing atau subversif.

b. Setiap warga PBU hendaklah mengambil langkah dan tindakan sewajarnya untuk memahami Akta Rahsia Rasmi 1972 bagi memastikan diri memahami dan sedar tanggungjawab masing-masing terhadap keselamatan di sisi undang-undang.

c. Setiap warga PBU adalah dikehendaki untuk menandatangani borang akuan Penjawat Awam berhubung Akta Rahsia Rasmi 1972 seperti di Lampiran D Arahan Keselamatan. Borang ini hendaklah ditandatangani setiap awal tahun sebagai peringatan.

d. Setiap warga juga dikehendaki menandatangani borang perakuan seperti di Lampiran E Arahan Keselamatan sebelum berhenti atau meninggalkan perkhidmatan Kerajaan.

e. Pekerja syarikat yang membekal perkhidmatan kepada PBU, seperti perkhidmatan kawalan keselamatan atau kebersihan, pula dikehendaki menandatangi borang akuan yang ditetapkan.

4.2 Tapisan Keselamatan

a. Pejabat Ketua Pegawai Keselamatan Kerajaan (PKPKK) adalah menjadi kuasa pusat mengenai dasar dan pengurusan tapisan keselamatan. Semua urusan tapisan keselamatan hendaklah dirujuk kepada PKPKK yang menjadi pihak berkuasa mengeluarkan sijil kelulusan tapisan keselamatan.

b. Kerajaan telah mewujudkan satu proses untuk memeriksa latar belakang penjawat awam yang dikenali sebagai Tapisan Keselamatan. Terdapat dua (2) jeins tapisan iaitu :

   i. **Tapisan Kasar** – proses asas yang digunakan bagi menapis penjawat awam yang dikehendaki melihat perkara-perkara terperingkat setakat peringkat SULIT

   ii. **Tapisan Halus** – proses yang teliti digunakan bagi menapis penjawat awam yang sentiasa dikehendaki melihat perkara terperingkat RAHSIA atau RAHSIA BESAR.

c. Warga PBU yang lulus Tapisan Keselamatan tidak berhak melihat semua perkara terperingkat secara automatik tetapi hanya setakat yang perlu untuk membolehkannya melaksanakan tanggungjawab atau kewajipannya sahaja.

d. Keputusan Tapisan Keselamatan perlu dicatat ke dalam Buku Perkhidmatan warga PBU yang berkenaan. Semua rekod keputusan hendaklah mengandungi rujukan serta tarikh surat keputusan tapisan keselamatan yang diperolehi dari PKPKK.

4.3 Prinsip “Perlu Mengetahui”

a. Perkara terperingkat, terutamanya Rahsia Besar dan Rahsia tidak boleh disampaikan kepada sesiapa selai daripada mereka yang betul-betul memerlukannya untuk menjalankan tugas. Staf PBU yang menguruskan perkara terperingkat Rahsia Besar hendaklah diasingkan. Prinsip “Perlu Mengetahui” hendaklah digunakan dalam apa keadaan sekalipun apabila menimbangkan soal penyampaian perkara terperingkat kepada orang lain.

b. Staf PBU dalam perkhidmatan sementara tidak dibenarkan akses kepada dokumen-dokumen terperingkat Rahsia Besar dan Rahsia. Staf sementara hanya boleh dibenarkan akses kepada dokumen Sulit dan Terhad dalam keadaan terkecualisahaja dengan kebenaran Pengarah.

c. Hanya staf PBU yang dibenarkan akses kepada dokumen terperingkat sahaja boleh menaip, menyalin atau meniru dokumen tersebut.

4.4 Pendidikan Keselamatan

a. Pendidikan merupakan asas kepada amalan keselamatan yang baik. Amalan dan pelaksanaan keselamatan perlindungan yang baik tidak akan tercapai sekiranya warga PBU tidak dididik untuk menerima dan mematuhi peraturan dan arahan keselamatan sebagai sebahagian daripada kewajipan biasa.

b. Pegawai Keselamatan Jabatan dikehendaki memastikan semua warga PBU diberi pendidikan keselamatan perlindungan yang sewajarnya, secara umum atau secara khusus, menggunakan kaedah-kaedah yang bersesuaian.

5.0 KESELAMATAN PENGGUNAAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

5.1 Pengenalan dan Objektif

Keselamatan Penggunaan Teknologi Maklumat dan Komunikasi (ICT) Politeknik Balik Pulau (PBU) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi. Keselamatan Penggunaan ICT ini juga memberi penerangan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT PBU.

Keselamatan Penggunaan ICT ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi PBU. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Objektif utama Keselamatan Penggunaan ICT PBU adalah seperti berikut:

i. Memastikan kelancaran operasi PBU dan meminimumkan kerosakan atau kemusnahan;

ii. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

iii. Mencegah salah guna atau kecurian aset ICT Kerajaan;

iv. Meminimumkan kos penyenggaraan ICT akibat ancaman dan penyalahgunaan; dan

v. Memperkemaskan pengurusan keselamatan ICT PBU.

5.2 Prinsip-Prinsip Asas kepada Keselamatan Penggunaan ICT PBU

Prinsip-prinsip yang menjadi asas kepada Keselamatan Penggunaan ICT PBU dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

Akses kepada penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

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, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses 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;

d. Pengasingan

Tugas mewujud, memadam, mengkemaskini, mengubah dan mengesah data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti 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 audit *trail*;

f. Pematuhan

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

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 aktiviti 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 mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

5.3 Keselamatan Capaian Pengguna

5.3.1 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:

a. Akaun yang diperuntukkan oleh PBU sahaja boleh digunakan;

b. Akaun pengguna mestilah unik dan mencerminkan identiti pengguna;

c. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan PBU. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan UICT boleh membeku dan menamatkan akaun pengguna atas sebab- sebab berikut:

   i. Bertukar bidang tugas kerja;

   ii. Bertukar ke agensi lain;

   iii. Bersara; atau

   iv. Ditamatkan perkhidmatan.

5.3.2 Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PBU seperti berikut:

a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

c. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

d. Kata laluan *Windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

e. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

f. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula;

g. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

h. Mengelakkan penggunaan semula kata laluan yang baru digunakan; dan

i. Penetapan kata laluan hendaklah mematuhi kombinasi panjang kata laluan sekurang- kurangnya lapan (8) aksara dengan gabungan huruf besar, huruf kecil, simbol dan angka.

Contoh: P@ssword.1234

5.3.3 Capaian Internet

a. Penggunaan internet di PBU adalah dipantau secara berterusan oleh UICT bagi memastikan penggunaannya adalah untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PBU;

b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. UICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;

c. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/Unit atau pegawai yang diberi kuasa;

d. Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan/Unit sebelum dimuat naik ke internet;

f. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

g. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PBU; dan

h. Pengguna adalah dilarang melakukan aktiviti- aktiviti seperti berikut:

   i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, audio yang boleh menjejaskan tahap capaian internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan bahan, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, perjudian atau keganasan.

5.3.4 Kawalan Kriptografi

Pengguna hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi.

5.3.5 *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* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer;

b. Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan

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

5.3.6 Backup

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Membuat salinan sandaran ke atas semua data dan maklumat mengikut keperluan. Kekerapan penduaan bergantung kepada tahap kritikal maklumat;

b. Melaksanakan salinan sandaran secara harian, mingguan, bulanan dan tahunan bergantung kepada tahap kritikal maklumat; dan

c. Pengguna hendaklah bertanggungjawab ke atas perlaksanaan salinan sandaran masing-masing.

5.4 Keselamatan Peralatan

Keselamatan peralatan adalah berkaitan dengan peraturan dan langkah-langkah bagi melindungi peralatan ICT PBU daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

5.4.1 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;

b. Pengguna bertanggungjawab sepenuhnya ke atas komputer/komputer riba masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran UICT;

e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

f. Pengguna mesti memastikan perisian antivirus di komputer/komputer riba yang dipertanggungjawabkan kepada pengguna sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan luaran yang digunakan;

g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

h. Peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS)

i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

k. Peralatan ICT yang hendak dibawa keluar dari premis PBU, perlulah mendapat kebenaran bertulis dari Pengarah atau pegawai yang diberi kuasa dan direkodkan seperti yang dinyatakan dalam pekeliling perbendaharaan sedia ada bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada Pengarah, PKJ dan Pegawai Aset dengan segera mengikut pekeliling perbendaharaan sedia ada;

m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

n. Pengguna tidak dibenarkan mengubah kedudukan komputer/komputer riba dari tempat asal ia ditempatkan tanpa kebenaran UICT;

o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada UICT untuk dibaik pulih;

p. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan;

r. Pengguna dilarang sama sekali mengguna dan mengubah kata laluan akaun pentadbir (*administrator password*) pada komputer/komputer riba yang dipertanggung- jawabkan dan telah ditetapkan;

s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

t. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat;

u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengarah PBU; dan

v. Semua pergerakan aset ICT PBU hendaklah direkodkan.

5.4.2 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *CDROM, thumb drive* dan media storan lain.

Langkah-langkah pencegahan seperti berikut hendaklah diambil bagi 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 adalah terhad kepada pegawai yang dibenarkan sahaja;

c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;

d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan;

e. Pergerakan media storan hendaklah direkodkan;

f. Perkakasan backup hendaklah diletakkan di tempat yang terkawal;

g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;

h. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu;

i. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat;

j. Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

5.4.3 Media Perisian Dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di PBU;

b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran UICT;

c. Lesen perisian (*registration code, serial numbers, CD-keys*) perlu disimpan berasingan daripada *CDROM*, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan

d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

5.4.4 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut perlu diambil untuk menjamin keselamatan perkakasan:

a. Peralatan yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai yang mengurus aset ICT dan tertakluk kepada tujuan yang dibenarkan;

b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan

c. Peralatan perlu dilindungi dan dikawal sepanjang masa;

d. Penyimpanan atau penempatan peralatan mestilah mengambil kira faktor keselamatan; dan

e. Kehilangan peralatan ICT perlu dilaporkan mengikut peraturan semasa yang ditetapkan.

5.5 Keselamatan Komunikasi

5.5.1 Pengurusan Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Mewujudkan prosedur kawalan pertukaran maklumat yang formal untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

b. Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PBU; dan

c. Melindungi sebaik-baiknya maklumat yang terdapat di dalam media.

5.5.2 Pengurusan Mel Elektronik

Penggunaan mel elektronik (e-mel) di PBU adalah dipantau secara berterusan oleh Pentadbir e-mel untuk memenuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam oleh Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Mengunakan akaun atau alamat e-mel yang diperuntukkan oleh PBU sahaja. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan;

c. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

d. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel;

e. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

f. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

g. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat serta mengambil tindakan segera; dan

h. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

5.5.3 Perkhidmatan Dalam Talian (*Online*)

Bagi menggalakkan pertumbuhan perkhidmatan dalam talian serta sebagai menyokong hasrat kerajaan mengoptimumkan penyampaian perkhidmatan melalui media elektronik, pengguna boleh menggunakan kemudahan internet.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Maklumat yang terlibat dalam transaksi dalam talian perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

b. Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan

c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

5.5.4 Media Sosial

Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut:

a. Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara;

b. Tidak melibatkan penyebaran maklumat dan dokumen terperingkat;

c. Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan;

d. Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan

e. Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.

5.6 Pengurusan Pengendalian Insiden Keselamatan ICT

5.6.1 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Keselamatan Penggunaan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Pengarah, PKJ dan Pasukan CERT JPPKK dengan kadar segera:

a. Maklumat didapati hilang atau 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 laluan atau mekanisme 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 komunikasi tersalah hantar; dan

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

Pelaporan insiden keselamatan ICT di PBU sepertimana Prosedur pelaporan insiden keselamatan ICT berdasarkan:

a. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

5.6.2 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang.

Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada PBU.

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;

b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

d. Menyediakan tindakan pemulihan segera; dan

e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

6.0 PENUTUP DAN TARIKH KUATKUASA GARIS PANDUAN

6.1 Adalah diharapkan Garis Panduan Keselamatan Perlindungan Politeknik Balik Pulau ini akan menjadi satu sumber rujukan penting dalam pengurusan dan pelaknsaan keselamatan perlindungan di Politeknik Balik Pulau.

6.2 Tarikh kuatkuasa Garis Panduan Keselamatan Perlindungan Politeknik Balik ini adalah pada **Oktober 2020**.

LAMPIRAN 1

TUGAS DAN TANGGUNGJAWAB PEGAWAI KESELAMATAN JABATAN

Ketua Jabatan adalah bertanggungjawab sepenuhnya mengenai keselamatan dalam Jabatannya seperti yang ditetapkan di Para 16 **Arahan Keselamatan Kerajaan**. Walaupun Ketua Jabatan bertanggungjawab sepenuhnya mengenai keselamatan dalam Jabatannya, beliau perlu melantik seorang Pegawai Kanan yang berkaliber untuk menyandang jawatan tersebut. Bertujuan untuk membantu beliau melaksanakan arahan-arahan keselamatan.

Pegawai Keselamatan Jabatan yang dilantik hendaklah terdiri daripada Timbalan Ketua Jabatan yang bertanggungjawab mengenai pentadbiran Jabatan untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan.

Tugas sebagai Pegawai Keselamatan Jabatan ini adalah sebagai tugas tambahan daripada tugas-tugas rasminya, meliputi: -

1. Bertanggungjawab ke atas semua aspek keselamatan dokumen dan maklumat rasmi Jabatan, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi selaras dengan peraturanperaturan yang ditetapkan oleh Kerajaan.

2. Mengemukakan perakuan-perakuan kepada Ketua Setiausaha Kementerian / Ketua Jabatan akan cadangan-cadangan untuk meningkatkan langkah-langkah Keselamatan Perlindungan dari semasa ke semasa mengikut kesesuaian.

3. Menubuhkan jawatankuasa keselamatan di Kementerian / Jabatan / Agensi Kerajaan yang dipengerusikan oleh Pegawai Keselamatan Jabatan berperanan untuk menyelaraskan pelaksanaan kawalan Keselamatan Perlindungan serta menyelesaikan isu-isu yang berbangkit dalam melaksanakan kawalan Keselamatan Perlindungan di Kementerian / Jabatan Kerajaan.

4. Mewakili Kementerian / Jabatan / Agensi Kerajaan dalam menghadiri mesyuarat mengenai keselamatan dari semasa ke semasa dan jika diperlukan hendaklah membentangkan laporan keselamatan kemeterian / Jabatan serta isu-isu yang tidak dapat diselesaikan di peringkat Kementerian / Jabatan.

5. Menubuhkan jawatankuasa yang akan dipengerusikan oleh Ketua Setiausaha Kementerian / Jabatan yang akan bermesyuarat dengan serta merta jika berlaku sebarang kejadian kecemasan yang melibatkan keselamatan dokumen dan kebocoran maklumat serta harta benda Kerajaan termasuk ancaman keselamatan, pencerobohan, kebakaran, kecurian dan sebagainya. Selanjutnya menyediakan laporan hasil mesyuarat jawatankuasa berkenaan untuk dikemukakan kepada pihak berkuasa berkenaan.

6. Mengadakan pemeriksaan dari semasa ke semasa ke atas bangunan, sistem pendawaian elektrik, bilik komputer, bilik dokumen dan peralatan, kawasan pejabat dan semua perkara di bawah tanggungjawabnya bagi mempastikan ia dalam keadaan yang selamat dan tidak terdedah kepada ancaman dan risiko.

7. Menganjurkan kursus dan taklimat kesedaran Keselamatan Perlindungan dengan kerjasama Pejabat Ketua Pegawai Keselamatan Kerajaan, Jabatan Perdana Menteri bagi mempastikan setiap anggota di Kementerian / Jabatan memahami langkah-langkah serta peraturanperaturan Keselamatan Perlindungan.

8. Berkerjasama rapat dengan Pegawai Keselamatan Kerajaan untuk mendapatkan khidmat nasihat mengenai langkah-langkah meningkatkan sistem dan kawalan Keselamatan Perlindungan di Kementerian / Jabatan.

9. Melaksanakan tugas-tugas lain yang ditetapkan dalam peraturan-peraturan keselamatan Kerajaan yang sedang berkuatkuasa dan yang dipinda dari semasa ke semasa.

LAMPIRAN 2

CONTOH-CONTOH PERINGKAT KESELAMATAN

Contoh-contoh penggunaan peringkat keselamatan berikut adalah sebagai panduan kepada penjawat awam yang memulakan perkara-perkara terperingkat. Peraturan berkaitan dengannya yang terkandung di dalam Arahan Keselamatan hendaklah dipatuhi apabila menentukan sesuatu peringkat keselamatan.

RAHSIA BESAR

i. Kertas-kertas Jemaah Menteri yang sangat penting mengenai dasar utama Kerajaan berkaitan dengan perkara politik atau ekonomi;

ii. Maklumat yang sangat penting mengenai perancangan gerakan dan penempatan barisan peperangan Angkatan Tentera jika berlaku peperangan;

iii. Surat menyurat dengan kerajaan negara asing mengenai aspek perdagangan dan pertahanan yang sangat penting;

iv. Maklumat lengkap berkenaan pertubuhan-pertubuhan perisikan Malaysia dan kaedah-kaedahnya.

RAHSIA

i. Arahan-arahan penting untuk perwakilan-perwakilan Malaysia yang membuat perundingan dengan negara asing;

ii. Maklumat-maklumat penting mengenai pemasangan-pemasangan tentera;

iii. Maklumat-maklumat penting mengenai pertubuhan-pertubuhan subversif dan kegiatan-kegiatannya;

iv. Surat menyurat antara jabatan mengenai perkara-perkara dasar penting.

SULIT

i. Laporan-laporan perisikan biasa;

ii. Dokumen-dokumen dan panduan-panduan teknik untuk kegunaan latihan tentera atau polis;

iii. Maklumat mengenai perkara-perkara perdagangan yang jika terdedah kepada orang yang tidak dibenarkan akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran dan Kerajaan;

iv. Maklumat-maklumat yang mengkin membolehkan pendapatan faedah kewangan daripadanya jika terdeah sebelum masa.

TERHAD

i. Buku-buku Jabatan bagi maksud arahan;

ii. Perintah-perintah dan arahan-arahan biasa Jabatan;

iii. Dokumen-dokumen mengenai bekalan barang-barang dan alat kelengkapan biasa untuk tentera atau polis.

GARIS PANDUAN KESELAMATAN PERLINDUNGAN

POLITEKNIK BALIK

Disediakan oleh :

Abdul Hanif Bin Mustapha
Pengarah
Politeknik Balik Pulau

Ts Hanim @ Zuraini Binti Talib
Pegawai Teknologi Maklumat
Politeknik Balik Pulau

Disemak oleh :

Ts Jasni Bin Mohd Yusoff
Timbalan Pengarah Akademik
Politeknik Balik Pulau

Mohd Yuhaizad Bin Yusoff
Timbalan Pengarah Sokongan Akademik
Politeknik Balik Pulau

Suzana Binti Saleh
Penolong Pegawai Tadbir
Politeknik Balik Pulau

Oktober 2020