DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

KETUA SETIAUSAHA
Secretary General
KEMENTERIAN PELAJARAN MALAYSIA
Ministry of Education Malaysia
ARAS 8, BLOK E8
KOMPLEKS E
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62604 PUTRAJAYA

Telefon : 03-8884 6069
Faks : 03-8888 5124
Laman Web: http://www.moe.gov.my

Rujukan Kami : KP.BPM(S).100-11/1/4 JLD 2 (61)
Tarikh : 19 Mac 2012

Semua Setiausaha / Pengarah Bahagian

Semua Pengarah Pelajaran Negeri

Kementerian Pelajaran Malaysia

PEKELILING ICT BIL. 1 TAHUN 2012

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (DKICT) KEMENTERIAN PELAJARAN MALAYSIA

TUJUAN

Pekeliling ICT ini bertujuan untuk menjelaskan Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) Kementerian Pelajaran Malaysia (KPM) versi 2.0 dan perkara-perkara berkaitan yang perlu dipatuhi dalam menggunakan aset ICT KPM.

LATAR BELAKANG

2. Pengemaskinian DKICT KPM dilakukan bagi memastikan dasar sentiasa seiring dengan keperluan penguatkuasaan kawalan dan langkah-langkah menyeluruh dalam melindungi Aset ICT Kerajaan.

3. Pekeliling ini dikeluarkan selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2009 bertajuk **"Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam"** yang dikeluarkan oleh Jabatan Perdana Menteri.

4. Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPM Bil.1/2012 yang telah diadakan pada 23 Februari 2012 telah bersetuju mengguna pakai dan menguatkuasakan peraturan-peraturan yang ditetapkan dalam pekeliling ini.

DASAR KESELAMATAN ICT

5. Dasar Keselamatan ICT mengambilkira objektif kawalan ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat yang meliputi perkara-perkara berikut:

- Dasar Keselamatan
- Organisasi Keselamatan Maklumat
- Pengurusan Aset
- Keselamatan Sumber Manusia
- Keselamatan Fizikal Dan Persekitaran
- Pengurusan Operasi Dan Komunikasi
- Kawalan Capaian
- Perolehan, Pembangunan Dan Penyelenggaraan Sistem Maklumat
- Pengurusan Insiden Keselamatan Maklumat
- Pengurusan Kesinambungan Perkhidmatan
- Pematuhan

TANGGUNGJAWAB BAHAGIAN/AGENSI

6. Semua Bahagian/Agensi dibawah KPM adalah dikehendaki mematuhi Pekeliling ICT Bil. 1 Tahun 2012 DKICT KPM dan melaksanakan tanggungjawab yang ditetapkan didalamnya.

PEMATUHAN

7. Semua pengguna ICT KPM adalah dikehendaki mematuhi DKICT KPM. Pematuhan merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran dasar.

PEMAKAIAN PEKELILING

8. Pekeliling ini dipanjangkan kepada semua Bahagian/Agensi dibawah KPM kecuali Dewan Bahasa dan Pustaka (DBP), Institut Terjemahan & Buku Malaysia (ITBM) dan Majlis Peperiksaan Malaysia (MPM).

TARIKH KUAT KUASA

9. Pekeliling ini berkuat kuasa mulai tarikh ia dikeluarkan.

PEMBATALAN

10. Dengan berkuat kuasanya Pekeliling ini, **Pekeliling ICT Bil. 1 Tahun 2009 Dasar Keselamatan ICT (DKICT) Kementerian Pelajaran Malaysia** adalah dibatalkan.

"BERKHIDMAT UNTUK NEGARA"

DATO' DR. ROSLI BIN MOHAMED
Ketua Setiausaha
Kementerian Pelajaran Malaysia

Salinan Kepada:

1. Ketua Pengarah Pelajaran Malaysia
2. Timbalan-Timbalan Ketua Setiausaha
   Kementerian Pelajaran Malaysia
3. Timbalan-Timbalan Ketua Pengarah Pelajaran
   Kementerian Pelajaran Malaysia
4. SUSK YAB Menteri Pelajaran Malaysia
5. SUSK YB Timbalan-Timbalan Menteri Pelajaran Malaysia

DASAR KESELAMATAN ICT
KEMENTERIAN PELAJARAN MALAYSIA
VERSI 2.0

MAC 2012

DKICT KPM

SEJARAH DOKUMEN

TARIKH	VERSI	PEKELILING	TARIKH KUATKUASA
23 Februari 2009	1.3	ICT BIL 1 TAHUN 2009	28 Februari 2009
23 Februari 2012	2.0	ICT BIL 1 TAHUN 2012	19 Mac 2012

KANDUNGAN **MUKASURAT**

11. KAWALAN CAPAIAN

TERMA DAN TAFSIRAN

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Ancaman	Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab KPM.
Backup	Proses penduaan data, maklumat, perisian sistem dan aplikasi.
CERT KPM	Pasukan Tindak Balas Insiden Keselamatan ICT KPM. (*Computer Emergency Response Team* KPM)
Dokumen	Semua himpunan atau kumpulan bahan yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Electronic Commerce	Perdagangan yang dijalankan secara internet.
Firewall	Perkakasan atau perisian atau kombinasi kedua-duanya yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman.
GCERT	Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. (*Government Computer Emergency Response Team*)

TERMA DAN TAFSIRAN

Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
ICT	Teknologi Maklumat dan Komunikasi. (*Information and Communications Technology*)
ICTSO	Pegawai Keselamatan ICT. (*Information & Communication Technology Security Officer*)
Integriti	Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.
IPS	Sistem Pencegah Pencerobohan. (*Intrusion Prevention System*) Perkakasan keselamatan rangkaian yang memantau aktiviti rangkaian yang berlaku dalam sistem bagi mengesan perisian berbahaya. Mampu bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*.
Ketersediaan	Data dan maklumat yang boleh diakses pada bila-bila masa.
Kerahsiaan	Maklumat yang tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
Keselamatan Maklumat	Pemeliharaan kerahsiaan, integriti dan ketersediaan maklumat, disamping sifat-sifat lain seperti kesahihan, akauntabiliti dan kebolehpercayaan.
KPM	Kementerian Pelajaran Malaysia.

TERMA DAN TAFSIRAN

Kriptografi	Penukaran data ke dalam kod rahsia untuk penghantaran melalui rangkaian awam.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious Code	Sebarang kod yang dicipta untuk merosakkan sistem atau data, atau untuk mencegah sistem daripada digunakan dengan cara yang biasa. Ia melibatkan skrip serangan, virus, cecacing, trojan horse, backdoors dan kandungan aktif yang berniat jahat.
Media Storan	Alat untuk menyimpan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
MyRAM	Metodologi Penilaian Risiko Keselamatan ICT Sektor Awam Malaysia. (*Malaysian Public Sector ICT Security Risk Assessment Methodology*)
Mobile Code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pengguna	Kakitangan KPM, pembekal, pakar runding dan pihak-pihak lain yang dibenarkan.

TERMA DAN TAFSIRAN

Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada KPM.
PRISMA	Pemantauan Rangkaian ICT Sektor Awam Malaysia.
Risiko	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
Router	Sejenis peralatan rangkaian yang digunakan untuk menghubungkan antara satu rangkaian dengan rangkaian yang lain.
Server	Pelayan Komputer.
SOP	*Standard Operating Procedure.*
WAN	*Wide Area Network* Rangkaian Kawasan Luas adalah rangkaian komputer jarak jauh dan menghubungkan kawasan yang lebih luas.

1. TUJUAN

Dasar ini bertujuan menerangkan peraturan-peraturan yang mesti dibaca, difahami dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Kementerian Pelajaran Malaysia (KPM).

2. SKOP

Dasar Keselamatan ICT KPM ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua aset ICT.

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KPM. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KPM;

c. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d. Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KPM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, profil-profil murid/pelajar, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain; dan

e. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif KPM. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

Setiap aset ICT perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

3. PRINSIP-PRINSIP

Prinsip-prinsip asas kepada Dasar Keselamatan ICT KPM dan perlu dipatuhi adalah seperti berikut:

a. Akses Atas Dasar Perlu Mengetahui
Akses terhadap 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. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. Hak Akses Minimum
Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses akan 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 KPM;

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

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan ICT atau mengenal pasti keadaan yang mengancam keselamatan ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan (*server*), *router, firewall, IPS, Antivirus* dan rangkaian hendaklah ditentukan supaya dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f. Pematuhan

Dasar Keselamatan ICT KPM 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 (*backup*) dan pewujudan 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 ICT yang maksimum.

4. PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Dasar Keselamatan ICT KPM merangkumi perlindungan kerahsiaan, integriti dan kebolehsediaan ke atas semua bentuk maklumat.

a. Maklumat hendaklah dilindungi dari pihak lain yang tidak diberi kuasa menggunakan maklumat;

b. Maklumat hendaklah sentiasa tepat, lengkap dan kemas kini semasa ianya diproses; dan

c. Maklumat hendaklah sentiasa tersedia jika diperlukan oleh pihak lain yang diberi kuasa mencapai maklumat tersebut.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

DASAR KESELAMATAN



5. DASAR KESELAMATAN

5.1 Dasar Keselamatan ICT

Objektif

Menyediakan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KPM dan perundangan serta peraturan yang berkaitan.

Dokumen Keselamatan ICT

5.1.1 Mendapat kelulusan Pengurusan Tertinggi KPM, menerbit dan menyebarkan kepada warga KPM dan pihak-pihak luar yang berkaitan.

Kajian Semula Dasar Keselamatan

5.1.2 Mengkaji semula setiap dua (2) tahun atau bila-bila masa sekiranya terdapat perubahan ketara bagi memastikan ianya bersesuaian, bertepatan dan efektif.

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

ORGANISASI KESELAMATAN MAKLUMAT

6. ORGANISASI KESELAMATAN MAKLUMAT

6.1 Pengurusan Keselamatan Maklumat

Objektif

Menguruskan keselamatan maklumat dalam organisasi.

6.1.1	Menyokong keselamatan dalam organisasi melalui hala tuju, penglibatan, tugasan, dan tanggungjawab yang jelas terhadap keselamatan maklumat.	Komitmen Pengurusan
6.1.2	Menyelaras aktiviti keselamatan maklumat oleh wakil-wakil dari Bahagian/Agensi KPM dengan peranan dan fungsi kerja yang berkaitan.	Penyelarasan Keselamatan Maklumat
6.1.3	Menyatakan dengan jelas peranan dan tanggungjawab semua keselamatan maklumat.	Peranan Dan Tanggungjawab Keselamatan Maklumat
6.1.4	Menentu dan melaksanakan proses kelulusan untuk kemudahan pemprosesan maklumat.	Kelulusan Untuk Kemudahan Pemprosesan Maklumat
6.1.5	Menyemak keperluan kerahsiaan atau *non-disclosure* dari semasa ke semasa bagi memastikan maklumat dilindungi dan tidak didedahkan sewenang-wenangnya.	Kerahsiaan Maklumat
6.1.6	Memastikan direktori pihak berkuasa berkaitan sentiasa dikemaskini.	Direktori Pihak Berkuasa Berkaitan
6.1.7	Memastikan direktori kumpulan berkepentingan seperti CERT KPM, GCERT, PRISMA sentiasa dikemaskini.	Direktori Kumpulan Berkepentingan

6.1.8 Mengkaji pengurusan keselamatan maklumat dan pelaksanaannya (objektif kawalan, kawalan, dasar, proses, dan prosedur keselamatan maklumat) oleh pihak ketiga pada tempoh masa yang dirancang, atau apabila perubahan yang besar kepada pelaksanaan keselamatan berlaku.

Kajian Keselamatan Maklumat Oleh Pihak Ketiga

6.2 Pihak Luar

Memastikan keselamatan maklumat dan kemudahan pemprosesan maklumat yang diakses, diproses, disampaikan kepada atau yang diuruskan oleh pihak luar.

Objektif

6.2.1 Mengenalpasti risiko dan mengambil tindakan kawalan terhadap maklumat dan kemudahan pemprosesan maklumat KPM yang melibatkan pihak luar sebelum akses dibenarkan.

Mengenalpasti Risiko Melibatkan Pihak Luar

6.2.2 Melaksanakan semua keperluan keselamatan yang telah dikenalpasti sebelum memberi kebenaran akses kepada maklumat atau aset ICT KPM.

Keperluan Keselamatan Bila Berurusan Dengan Pengguna

6.2.3 Memastikan semua keperluan keselamatan yang berkaitan dinyatakan dengan jelas dalam semua kontrak perjanjian yang melibatkan akses, pemprosesan, penghantaran maklumat, atau kemudahan pemprosesan maklumat KPM atau tambahan peralatan atau perkhidmatan oleh pihak luar.

Keperluan Keselamatan Dalam Perjanjian Pihak Ketiga

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PENGURUSAN ASET

7. PENGURUSAN ASET

7.1 Akauntabiliti Aset

	Memastikan perlindungan yang sesuai ke atas semua aset ICT KPM.	Objektif
7.1.1	Mengenalpasti, mendaftar dan menyelenggara inventori semua aset ICT.	Inventori Aset ICT
7.1.2	Memastikan pemilikan dan pengurusan semua maklumat dan aset ICT dipertanggungjawabkan kepada pihak-pihak yang berkenaan.	Pemilikan Aset ICT
7.1.3	Memastikan semua peraturan yang membenarkan penggunaan maklumat dan aset ICT dikenalpasti, didokumen dan dilaksanakan.	Kebenaran Menggunakan Aset ICT

7.2 Pengkelasan Maklumat

	Memastikan semua maklumat diberi perlindungan mengikut tahap keselamatan.	Objektif
7.2.1	Memastikan maklumat dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada KPM.	Pengkelasan Maklumat
7.2.2	Menyedia dan melaksanakan prosedur yang sesuai bagi pelabelan dan pengendalian maklumat mengikut klasifikasi yang digunapakai oleh KPM.	Pelabelan Dan Pengendalian Maklumat

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

KESELAMATAN SUMBER MANUSIA



8. KESELAMATAN SUMBER MANUSIA

8.1 Sebelum Perkhidmatan

Objektif

Memastikan warga KPM, kontraktor dan pihak ketiga memahami peranan dan tanggungjawab mereka bagi mengurangkan risiko kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan.

Peranan Dan Tanggungjawab

8.1.1 Menyatakan dengan jelas peranan dan tanggungjawab warga KPM, kontraktor dan pihak ketiga terhadap keselamatan ICT selaras dengan Dasar Keselamatan ICT.

Verifikasi

8.1.2 Melaksanakan pengesahan identiti ke atas warga KPM, kontraktor dan pihak ketiga selaras dengan peruntukan perundangan dan peraturan yang berkaitan keperluan perkhidmatan dan peringkat maklumat yang hendak dicapai serta risiko yang dijangkakan.

Terma Dan Syarat-Syarat Kontrak

8.1.3 Mematuhi semua terma dan syarat-syarat dalam kontrak yang ditawarkan dan peraturan semasa yang berkuatkuasa bagi kontraktor dan pihak ketiga.

8.2 Semasa Perkhidmatan

Objektif

Memastikan warga KPM, kontraktor dan pihak ketiga sedar dan mengambil berat akan ancaman keselamatan aset ICT, serta tanggungjawab dan liabiliti dalam menjalankan tugas harian dan mengurangkan risiko kesilapan manusia.

8.2.1	Memastikan warga KPM, kontraktor dan pihak ketiga melaksanakan tanggungjawab keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh KPM.	Tanggungjawab Pengurusan
8.2.2	Memastikan warga KPM, kontraktor dan pihak ketiga, (di mana berkaitan) diberi pendedahan mengenai dasar dan prosedur keselamatan yang berkaitan dengan bidang tugas dari semasa ke semasa.	Kesedaran Keselamatan Maklumat
8.2.3	Memastikan adanya proses tindakan disiplin ke atas warga KPM yang melanggar peraturan keselamatan.	Proses Disiplin

8.3 Bertukar atau Tamat Perkhidmatan

	Memastikan warga KPM, kontraktor dan pihak ketiga yang bertukar atau tamat perkhidmatan diurus dengan teratur.	Objektif
8.3.1	Memastikan tugas pegawai yang bertanggungjawab menguruskan pertukaran atau penamatan perkhidmatan dinyatakan dengan jelas.	Tanggungjawab Pegawai
8.3.2	Memastikan warga KPM, kontraktor dan pihak ketiga yang bertukar atau tamat perkhidmatan menyerahkan aset ICT KPM.	Pemulangan Aset
8.3.3	Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat bagi warga KPM, kontraktor dan pihak ketiga yang bertukar atau tamat perkhidmatan.	Pembatalan Hak Capaian

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

KESELAMATAN FIZIKAL DAN PERSEKITARAN

9. KESELAMATAN FIZIKAL DAN PERSEKITARAN

9.1 Keselamatan Kawasan

Objektif

Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan ancaman kepada premis dan maklumat.

9.1.1 Melaksanakan kawalan keselamatan untuk melindungi kawasan yang menyimpan maklumat dan kemudahan pemprosesan maklumat.

Keselamatan Perimeter

9.1.2 Melindungi kawasan larangan / kawasan keselamatan bagi memastikan kakitangan yang dibenarkan sahaja diberi akses.

Kawalan Masuk Fizikal

9.1.3 Merekabentuk dan melaksanakan keselamatan fizikal untuk pejabat, bilik-bilik dan kemudahan yang disediakan.

Keselamatan Pejabat, Bilik Dan Kemudahan

9.1.4 Merekabentuk dan melaksanakan perlindungan fizikal dari kerosakan akibat kebakaran, banjir, gempa bumi, letupan, rusuhan awam dan lain-lain bencana alam atau bencana buatan manusia.

Perlindungan Terhadap Ancaman Luar Dan Persekitaran

9.1.5 Menyediakan garis panduan bagi mereka yang bertugas di kawasan keselamatan.

Bekerja Di Kawasan Keselamatan

9.1.6 Mengawal laluan akses bagi kawasan penghantaran dan pemunggahan serta lain-lain laluan akses untuk mengelakkan akses yang tidak dibenarkan.

Laluan Akses Awam, Penghantaran Dan Pemunggahan

9.2 Keselamatan Peralatan

Objektif

Mencegah kehilangan, kerosakan, kecurian atau salah guna aset dan gangguan kepada aktiviti-aktiviti organisasi.

Penempatan Dan Perlindungan Peralatan

9.2.1 Menempatkan atau melindungi peralatan untuk mengurangkan risiko ancaman persekitaran dan bencana alam serta peluang-peluang akses yang tidak dibenarkan.

Kemudahan Sokongan

9.2.2 Melindungi peralatan ICT dari kegagalan bekalan kuasa dan lain-lain gangguan yang disebabkan oleh kegagalan kemudahan sokongan.

Keselamatan Kabel

9.2.3 Melindungi kabel elektrik dan telekomunikasi dari pemintasan dan kerosakan.

Penyelenggaraan Peralatan

9.2.4 Menyelenggara peralatan dengan teratur bagi memastikan integriti dan ketersediaan yang berterusan.

Keselamatan Peralatan Di Luar Premis

9.2.5 Mengambil langkah keselamatan ke atas peralatan yang dibawa keluar dari premis organisasi.

Pelupusan Atau Penggunaan Semula Peralatan

9.2.6 Menyemak semua peralatan yang mengandungi media storan untuk memastikan data yang sensitif dan perisian berlesen dihapuskan sebelum dilupus.

Aset ICT Yang Dibawa Keluar

9.2.7 Mendapatkan kebenaran terlebih dahulu sebelum peralatan, maklumat atau perisian dibawa keluar dari premis organisasi.

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PENGURUSAN OPERASI DAN KOMUNIKASI



10. PENGURUSAN OPERASI DAN KOMUNIKASI

10.1 Prosedur Operasi Dan Tanggungjawab

Objektif

Memastikan kemudahan pemprosesan maklumat beroperasi dengan betul dan selamat.

Mendokumenkan Prosedur Operasi

10.1.1 Mendokumen, menyelenggara prosedur operasi dan tersedia untuk semua pengguna yang memerlukan.

Pengurusan Perubahan

10.1.2 Mengawal semua perubahan kepada sistem dan kemudahan pemprosesan maklumat.

Pengagihan Tugas

10.1.3 Mengagihkan tugas dan tanggungjawab secara berasingan untuk mengurangkan peluang bagi ubahsuai tanpa kebenaran atau tidak disengajakan atau salah guna aset KPM.

Pengasingan Kemudahan Pembangunan, Pengujian Dan Pengoperasian

10.1.4 Mengasingkan kemudahan pembangunan, ujian dan operasi bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada sistem yang sedang beroperasi.

10.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif

Melaksana dan memastikan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan kontrak perkhidmatan pihak ketiga.

10.2.1	Memastikan tahap kawalan keselamatan, jenis dan penyampaian perkhidmatan yang terkandung dalam kontrak perkhidmatan pihak ketiga dipatuhi dan dilaksanakan.	Penyampaian Perkhidmatan
10.2.2	Memantau perkhidmatan dan menyemak laporan dan rekod yang disediakan oleh pihak ketiga serta melaksanakan audit secara berkala.	Memantau Dan Menyemak Perkhidmatan Pihak Ketiga
10.2.3	Mengurus sebarang perubahan terhadap pembekalan perkhidmatan dengan mengambil kira tahap kritikal perkhidmatan dan proses yang terlibat serta melaksanakan penilaian semula risiko keselamatan.	Mengurus Perubahan Kepada Perkhidmatan Pihak Ketiga

10.3 Perancangan Dan Penerimaan Sistem

	Meminimumkan risiko kegagalan sistem.	Objektif
10.3.1	Memantau, melaksanakan penalaan dan membuat unjuran keperluan sumber bagi memenuhi tahap prestasi yang ditetapkan.	Pengurusan Kapasiti
10.3.2	Menetapkan kriteria penerimaan dan menjalankan ujian bagi sistem baru, sistem yang dipertingkatkan dan versi baru semasa pembangunan dan sebelum penerimaan.	Penerimaan Sistem

10.4 Perlindungan Dari Kod Jahat (*Malicious Code*) Dan Kod Mudah Alih (*Mobile Code*)

	Melindungi integriti perisian dan maklumat.	Objektif

10.4.1 Melaksanakan kawalan pengesanan, pencegahan dan pemulihan untuk melindungi dari kod jahat dan melaksanakan prosedur kesedaran pengguna yang sesuai.

Kawalan Terhadap Kod Jahat

10.4.2 Melaksanakan konfigurasi bagi memastikan kod mudah alih yang dibenarkan beroperasi selaras dengan dasar keselamatan yang ditetapkan.

Kawalan Terhadap Kod Mudah Alih

10.5 *Backup*

Mengekalkan integriti dan ketersediaan maklumat dan kemudahan pemprosesan maklumat.

Objektif

10.5.1 Melaksanakan *backup* maklumat dan perisian serta melakukan ujian secara berkala selaras dengan prosedur *backup* yang ditetapkan.

Backup Maklumat

10.6 Pengurusan Keselamatan Rangkaian

Memastikan maklumat dalam rangkaian dan infrastruktur sokongan dilindungi.

Objektif

10.6.1 Mengawal dan mengurus rangkaian dengan baik, untuk melindungi dari ancaman dan menjamin keselamatan sistem dan aplikasi.

Kawalan Rangkaian

10.6.2 Mengenalpasti dan memasukkan ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan semua perkhidmatan rangkaian ke dalam kontrak perkhidmatan rangkaian.

Keselamatan Perkhidmatan Rangkaian

10.7 Pengendalian Media

Objektif

Melindungi media yang mengandungi maklumat dari sebarang pendedahan, pengubahsuaian dan penghapusan atau pemusnahan yang tidak dibenarkan.

10.7.1 Mewujudkan prosedur bagi pengurusan media mudah alih.

Pengurusan Media Mudah Alih

10.7.2 Melupuskan media yang tidak diperlukan secara selamat dan terjamin mengikut prosedur yang ditetapkan.

Pelupusan Media

10.7.3 Mewujudkan prosedur pengendalian dan penyimpanan maklumat untuk melindungi maklumat dari didedahkan tanpa kebenaran atau disalah guna.

Prosedur Pengendalian Maklumat

10.7.4 Melindungi dokumentasi sistem daripada capaian yang tidak dibenarkan.

Keselamatan Dokumentasi Sistem

10.8 Pertukaran Maklumat

Objektif

Menjamin keselamatan pertukaran maklumat dan perisian dalam KPM dan dengan mana-mana agensi luar.

10.8.1 Mewujudkan dasar, prosedur dan kawalan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai kemudahan komunikasi.

Prosedur Dan Dasar Pertukaran Maklumat

10.8.2 Menyediakan persetujuan pertukaran maklumat dan perisian dalam KPM dan dengan agensi luar.

Persetujuan Pertukaran

10.8.3	Melindungi media mengandungi maklumat daripada didedahkan, disalahguna atau dirosakkan kepada mereka yang tidak dibenarkan semasa pemindahan keluar dari KPM.	Media Dalam Transit
10.8.4	Melindungi maklumat yang terdapat dalam mesej elektronik.	Mesej Elektronik
10.8.5	Menyedia dan melaksana dasar dan prosedur bagi melindungi maklumat yang terlibat dalam pertukaran maklumat antara sistem.	Pertukaran Maklumat Antara Sistem

10.9 Perkhidmatan *Electronic Commerce*

	Memastikan keselamatan perkhidmatan *Electronic Commerce* dan penggunaannya selamat.	Objektif
10.9.1	Melindungi maklumat yang terlibat dalam transaksi elektronik menggunakan rangkaian awam daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan.	Transaksi Elektronik
10.9.2	Melindungi maklumat yang terlibat dengan transaksi dalam talian (*on-line*) bagi mengelak transmisi tidak lengkap, salah destinasi, dan pengubahsuaian, pendedahan, penduaan atau pengulangan mesej yang tidak dibenarkan.	Transaksi *On-Line*
10.9.3	Melindungi integriti maklumat yang disediakan pada sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan dari pengubahsuaian yang tidak dibenarkan.	Maklumat Awam

10.10 Pemantauan

Objektif

Mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan.

Log Audit

10.10.1 Menghasil dan menyimpan Log Audit yang merekodkan semua aktiviti untuk tempoh masa yang ditetapkan bagi memantau kawalan capaian dan membantu siasatan pada masa hadapan.

Pemantauan Penggunaan Sistem

10.10.2 Mewujudkan prosedur untuk memantau penggunaan kemudahan pemprosesan maklumat dan hasil pemantauan dikaji dari semasa ke semasa.

Perlindungan Maklumat Log

10.10.3 Melindungi kemudahan dan maklumat log daripada dipinda dan capaian yang tidak dibenarkan.

Log Pentadbir Dan Operator

10.10.4 Memastikan aktiviti pentadbir dan operator sistem direkodkan (*Logged*).

Log Kesalahan Dan Kesilapan

10.10.5 Memastikan sebarang kesilapan dilog, dianalisis dan diambil tindakan sewajarnya.

Keseragaman Waktu Sistem

10.10.6 Menyeragam waktu bagi semua sistem pemprosesan maklumat dalam KPM atau domain keselamatan dengan sumber waktu yang ditetapkan.

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

KAWALAN CAPAIAN

11. KAWALAN CAPAIAN

11.1 Keperluan Kawalan Capaian

Mengawal capaian maklumat. — Objektif

11.1.1 Mewujud, mendokumen dan mengkaji dasar kawalan berasaskan keperluan perkhidmatan dan keselamatan capaian. — Peraturan Kawalan Capaian

11.2 Pengurusan Capaian Pengguna

Memastikan capaian pengguna yang dibenarkan dan menghalang capaian pengguna yang tidak dibenarkan ke atas sistem maklumat. — Objektif

11.2.1 Mewujudkan prosedur pendaftaran dan pembatalan pendaftaran pengguna untuk memberi kebenaran dan membatalkan capaian ke atas semua sistem maklumat dan perkhidmatan yang disediakan. — Pendaftaran Pengguna

11.2.2 Mengawal dan menghadkan pengagihan dan penggunaan hak istimewa. — Pengurusan Hak Istimewa

11.2.3 Mengawal pengagihan kata laluan melalui proses yang ditetapkan. — Pengurusan Kata Laluan Pengguna

11.2.4 Mengkaji hak capaian pengguna dari semasa ke semasa melalui saluran yang ditetapkan. — Semakan Semula Hak Capaian Pengguna

11.3 Tanggungjawab Pengguna

Objektif

Menghalang salah guna atau kecurian maklumat dan kemudahan pemprosesan maklumat serta capaian pengguna yang tidak dibenarkan.

Penggunaan Kata Laluan

11.3.1 Memastikan pengguna mengikut amalan terbaik dalam pemilihan dan penggunaan kata laluan.

Peralatan Tanpa Kehadiran Pengguna (*Unattended User Equipment*)

11.3.2 Memastikan peralatan tanpa kehadiran pengguna mempunyai perlindungan yang sesuai.

Clear Desk Dan *Clear Screen*

11.3.3 Menggunapakai dasar *Clear Desk* untuk kertas dan media storan mudah-alih dan dasar *Clear Screen* untuk kemudahan pemprosesan maklumat.

11.4 Kawalan Capaian Rangkaian

Objektif

Menghalang capaian yang tidak dibenarkan ke atas perkhidmatan rangkaian.

Peraturan Penggunaan Perkhidmatan Rangkaian

11.4.1 Menyediakan kebenaran capaian ke atas perkhidmatan yang dibenarkan sahaja.

Pengesahan Pengguna Luar

11.4.2 Menggunakan kaedah pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh (*remote access*).

Pengenalan Peralatan Dalam Rangkaian

11.4.3 Menggunakan peralatan automatik berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian.

Remote Diagnostic Dan Perlindungan Konfigurasi

11.4.4 Mengawal capaian fizikal dan logikal ke atas kemudahan diagnostik dan konfigurasi.

11.4.5 Mengasingkan capaian mengikut kumpulan perkhidmatan, pengguna dan sistem maklumat. — Pengasingan Dalam Rangkaian

11.4.6 Menghadkan keupayaan pengguna untuk kemudahan sambungan bagi rangkaian yang dikongsi khususnya yang menjangkau sempadan KPM, selaras dengan dasar kawalan capaian dan keperluan aplikasi. — Kawalan Sambungan Rangkaian

11.4.7 Melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan bahawa sambungan komputer dan aliran maklumat tidak melanggar dasar kawalan capaian bagi setiap aplikasi. — Kawalan Laluan Rangkaian

11.5 Kawalan Capaian Sistem Pengoperasian

Mengelakkan capaian tanpa kebenaran ke atas sistem pengoperasian. — Objektif

11.5.1 Mengawal capaian kepada sistem pengoperasian menggunakan prosedur *log-on* yang selamat. — Prosedur *Log-On* Yang Selamat

11.5.2 Menyediakan pengenalan diri (*user ID*) yang unik dan teknik pengesahan yang sesuai untuk menjamin ketulenan pengguna. — Pengenalan Dan Pengesahan Pengguna

11.5.3 Menyediakan sistem pengurusan kata laluan dan memastikan kualiti kata laluan. — Sistem Pengurusan Kata Laluan

11.5.4 Menghad dan mengawal penggunaan program utiliti yang berkeupayaan melepasi kawalan sistem dan aplikasi. — Penggunaan Utiliti Sistem

11.5.5 Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan. — Sesi *Time-Out*

11.5.6	Menghadkan tempoh masa sambungan ke aplikasi yang berisiko tinggi.	Had Masa Sambungan

11.6 Kawalan Capaian Aplikasi Dan Maklumat

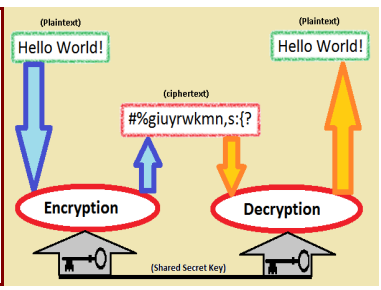
	Menghalang capaian tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	Objektif
11.6.1	Menghadkan capaian ke atas maklumat dan fungsi-fungsi sistem aplikasi oleh pengguna dan personel sokongan, selaras dengan dasar kawalan capaian yang ditetapkan.	Kawalan Capaian Maklumat
11.6.2	Mewujudkan persekitaran pengkomputeran yang khusus (terasing) bagi sistem yang sensitif.	Pengasingan Sistem Sensitif

11.7 Peralatan Mudah Alih Dan *Teleworking*

	Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan *teleworking*.	Objektif
11.7.1	Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi.	Peralatan Mudah Alih Dan Komunikasi
11.7.2	Merangka dan melaksana dasar, peraturan dan garis panduan bagi aktiviti *teleworking*.	*Teleworking*

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT



12. PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

12.1 Keperluan Keselamatan Sistem Maklumat

Memastikan keselamatan disepadukan dalam sistem maklumat.

Objektif

12.1.1 Menentukan keperluan kawalan keselamatan bagi sistem maklumat baru atau sistem maklumat sedia ada yang dipertingkatkan.

Spesifikasi Dan Analisis Keperluan Keselamatan

12.2 Pemprosesan Yang Betul Dalam Aplikasi

Mencegah kesilapan, kehilangan, pengubahsuaian tanpa kebenaran atau salahguna maklumat dalam aplikasi.

Objektif

12.2.1 Menentusahkan data input ke aplikasi bagi memastikan data yang dimasukkan betul dan bersesuaian.

Pengesahan Data *Input*

12.2.2 Memasukkan semakan pengesahan (*validation*) ke dalam aplikasi untuk mengesan kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan.

Kawalan Prosesan Dalaman

12.2.3 Mengenalpasti keperluan bagi memastikan kesahihan dan perlindungan integriti mesej dalam aplikasi dan kawalan yang sesuai dilaksanakan.

Mesej Integriti

12.2.4 Menentusahkan data *output* daripada aplikasi bagi memastikan pemprosesan penyimpanan maklumat yang dihasilkan adalah betul dan sesuai.

Pengesahan Data *Output*

12.3 Kawalan Kriptografi

Melindungi kerahsiaan, integriti atau kesahihan maklumat melalui kaedah kriptografi. — Objektif

12.3.1 Menyedia dan melaksanakan peraturan mengenai penggunaan kaedah kriptografi bagi melindungi maklumat. — Peraturan Penggunaan Kriptografi

12.3.2 Mengadakan pengurusan infrastruktur kunci awam yang menyokong teknik kriptografi. — Pengurusan Infrastruktur Kunci Awam

12.4 Keselamatan Fail-Fail Sistem

Memastikan keselamatan fail-fail sistem. — Objektif

12.4.1 Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam persekitaran operasi. — Kawalan Operasi Perisian

12.4.2 Memilih data ujian dengan teliti, dilindungi dan dikawal. — Perlindungan Data Ujian

12.4.3 Menghadkan capaian ke atas kod sumber program. — Kawalan Capaian Kod Sumber

12.5 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Memastikan keselamatan perisian sistem aplikasi dan maklumat. — Objektif

12.5.1 Menggunakan prosedur kawalan perubahan untuk mengawal pelaksanaan perubahan. — Prosedur Kawalan Perubahan

12.5.2 Mengkaji semula dan menguji aplikasi kritikal apabila terdapat perubahan terhadap sistem pengoperasian untuk memastikan tiada kesan buruk terhadap operasi KPM atau keselamatan.

Kajian Semula Aplikasi Selepas Perubahan Sistem Pengoperasian

12.5.3 Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan sebarang perubahan adalah terhad mengikut keperluan sahaja.

Kawalan Perubahan Pakej Perisian

12.5.4 Menghalang sebarang kemungkinan berlaku kebocoran maklumat.

Kebocoran Maklumat

12.5.5 Menyelia dan memantau pembangunan perisian yang dilaksanakan secara *outsourced*.

Pembangunan Perisian Secara *Outsourced*

12.6 Pengurusan Keterdedahan (*Vulnerability*) Teknikal

Objektif

Mengurangkan risiko akibat daripada eksploitasi keterdedahan teknikal.

12.6.1 Memperoleh maklumat yang cepat mengenai keterdedahan teknikal sistem maklumat, menilai keterdedahan, dan mengambil langkah-langkah yang sesuai untuk menangani risiko yang berkaitan.

Kawalan Keterdedahan Teknikal

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

13. PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

13.1 Pelaporan Insiden Dan Kelemahan Keselamatan Maklumat

Objektif

Memastikan insiden dan kelemahan keselamatan maklumat yang berkaitan dengan sistem maklumat disalurkan dengan cara yang membolehkan tindakan pembetulan diambil dengan segera.

Pelaporan Insiden Keselamatan Maklumat

13.1.1 Melaporkan insiden keselamatan maklumat kepada CERT KPM dengan kadar segera.

Pelaporan Kelemahan Keselamatan

13.1.2 Memastikan semua warga KPM, kontraktor dan pihak ketiga melaporkan kepada CERT KPM sebarang pemerhatian atau kelemahan keselamatan semasa menggunakan sistem maklumat dan perkhidmatan yang disediakan.

13.2 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat

Objektif

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan insiden keselamatan maklumat.

Tanggungjawab Dan Prosedur

13.2.1 Mewujudkan CERT KPM dan prosedur bagi memastikan tindakan insiden keselamatan maklumat dikendalikan dengan cepat, berkesan dan teratur.

Pengajaran Dari Insiden Keselamatan Maklumat

13.2.2 Mewujudkan mekanisma bagi membolehkan jenis, jumlah dan kos insiden keselamatan maklumat dinilai dan dipantau.

13.2.3 Mengumpul, menyimpan, dan menyerahkan bahan-bahan bukti mengikut peraturan-peraturan yang ditetapkan di bawah bidang kuasa perundangan yang berkaitan, sekiranya tindakan susulan terhadap orang atau organisasi selepas sesuatu insiden keselamatan maklumat (sama ada sivil atau jenayah).

Pengumpulan Bahan Bukti

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

14. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

14.1 Aspek-aspek Keselamatan Maklumat Pengurusan Kesinambungan Perkhidmatan

Memastikan fungsi-fungsi kritikal perkhidmatan sistem dan proses-proses utama dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.

Objektif

14.1.1 Menyedia dan menyenggara proses kerja bagi kesinambungan perkhidmatan dengan mengambil kira keperluan keselamatan maklumat.

Aspek-aspek Keselamatan Maklumat Dalam Proses Pengurusan Kesinambungan Perkhidmatan

14.1.2 Mengenalpasti insiden-insiden yang boleh mengakibatkan gangguan kepada perkhidmatan bersama dengan kemungkinan dan kesan terhadap keselamatan maklumat.

Kesinambungan Perkhidmatan Dan Penilaian Risiko

14.1.3 Membangun dan melaksana pelan kesinambungan perkhidmatan untuk mengekalkan atau memulihkan operasi dan memastikan ketersediaan maklumat di peringkat yang diperlukan dalam skala masa yang ditetapkan berikutan dari gangguan atau kegagalan, proses-proses perkhidmatan kritikal.

Membangun Dan Melaksanakan Pelan Kesinambungan Termasuk Keselamatan Maklumat

14.1.4 Menetapkan satu rangka kerja pelan kesinambungan perkhidmatan bagi memastikan semua pelan adalah konsisten dan sentiasa mengambil kira keperluan keselamatan maklumat.

Rangka Kerja Perancangan Kesinambungan Perkhidmatan

14.1.5 Memastikan Pelan Kesinambungan Perkhidmatan diuji dan dikemaskini secara berkala supaya ia sentiasa terkini.

Menguji, Menyelenggara Dan Menilai Semula Pelan Kesinambungan Perkhidmatan

DASAR KESELAMATAN ICT (DKICT) VERSI 2.0
KEMENTERIAN PELAJARAN MALAYSIA

PEMATUHAN

15. PEMATUHAN

15.1 Mematuhi Keperluan Perundangan

Objektif

Mengelak pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak, dan apa-apa keperluan keselamatan.

Pengenalan Undang-Undang Terpakai

15.1.1 Menentu, mendokumen dan menyimpan semua keperluan perundangan dan peraturan KPM yang terkini.

Hak Harta Intelek (IPR)

15.1.2 Melaksanakan prosedur yang bersesuaian bagi memastikan pematuhan kepada keperluan perundangan dan peraturan dalam penggunaan bahan yang mempunyai hak harta intelek dan penggunaan produk-produk perisian *proprietary*.

Perlindungan Rekod Organisasi

15.1.3 Melindungi rekod-rekod penting daripada kehilangan, kemusnahan dan pemalsuan, mengikut keperluan perundangan, peraturan dan perkhidmatan.

Perlindungan Data Dan Privasi Maklumat Peribadi

15.1.4 Memastikan perlindungan data dan privasi maklumat peribadi mematuhi peraturan-peraturan, dan klausa-klausa perundangan yang berkaitan.

Pencegahan Penyalahgunaan Kemudahan Pemprosesan Maklumat

15.1.5 Menghalang pengguna daripada menggunakan kemudahan pemprosesan maklumat untuk tujuan yang tidak dibenarkan.

Peraturan Kawalan Kriptografi

15.1.6 Menggunakan kawalan kriptografi berpandukan perjanjian, perundangan dan peraturan yang berkaitan.

15.2 Pematuhan Dasar Keselamatan dan Piawaian, Dan Pematuhan Teknikal

Objektif

Memastikan pematuhan sistem dengan dasar keselamatan dan piawaian KPM.

15.2.1 Memastikan ketua jabatan melaksanakan prosedur keselamatan yang ditetapkan dalam dasar keselamatan dan piawaian.

Pematuhan Dengan Dasar Keselamatan Dan Piawaian

15.2.2 Memeriksa sistem maklumat secara berkala terhadap pematuhan keselamatan dan piawaian.

Pematuhan Pemeriksaan Teknikal

15.3 Audit Sistem Maklumat

Objektif

Memaksimumkan keberkesanan dan meminimumkan gangguan kepada/daripada sistem maklumat.

15.3.1 Merancang dan mempersetujui keperluan audit dan aktiviti-aktiviti yang melibatkan pemeriksaan sistem yang sedang beroperasi bagi meminimakan gangguan kepada perkhidmatan.

Kawalan Audit Sistem Maklumat

15.3.2 Melindungi *audit tools* sistem maklumat bagi mencegah sebarang penyalahgunaan.

Perlindungan *Audit Tools* Sistem Maklumat

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT
KEMENTERIAN PELAJARAN MALAYSIA

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Bahagian / Jabatan : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan–peruntukan yang terkandung di dalam Dasar Keselamatan ICT KPM; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : ……

Tarikh : ……

Pengesahan Ketua Jabatan / Bahagian

……...

( )

b.p Ketua Setiausaha

Kementerian Pelajaran Malaysia

Tarikh : ……

LAMPIRAN B

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan
2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002
4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006
9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007
10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007
11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)
12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender
13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan
14. Akta Tandatangan Digital 1997
15. Akta Rahsia Rasmi 1972
16. Akta Jenayah Komputer 1997
17. Akta Hak Cipta (Pindaan) Tahun 1997
18. Akta Komunikasi dan Multimedia 1998

19. Perintah-Perintah Am
20. Arahan Perbendaharaan
21. Arahan Teknologi Maklumat 2007
22. Garis Panduan Keselamatan MAMPU 2004
23. Standard Operating Procedure (SOP) ICT KPM
24. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009
25. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010
26. Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam yang bertarikh 24 November 2010