MDKS

DERAF DASAR KESELAMATAN ICT (DKICT)
MAJLIS DAERAH KUALA SELANGOR

VersI 2.0

8 MEI 2015

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
1 September 2010	1.0	(6) dlm MDKS 146/6-11 22 September 2010	28 September 2010

JADUAL PINDAAN DASAR KESELAMATAN ICT MDKS

TARIKH	VERSI	BUTIR PINDAAN
7 Mei 2015	**2.0**	**a) Perkara DM-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga,** muka surat 27/90 : g) Menandatangani *Non Disclosure Agreement (NDA)* sebagaimana **Lampiran D.**

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT MDKS (DKICT MDKS) merangkumi Dasar Keselamatan ICT Majlis Daerah Kuala Selangor dan semua cawangan dibawahnya. Dasar ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Majlis Daerah Kuala Selangor (MDKS). Dasar ini juga menerangkan kepada semua pengguna di MDKS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MDKS.

OBJEKTIF

DKICT MDKS diwujudkan untuk menjamin kesinambungan urusan pengoperasian dan pengurusan ICT MDKS dengan meminimumkan kesan insiden keselamatan ICT MDKS

Objektif utama DKICT MDKS ialah seperti berikut :-

a) Memastikan kelancaran pengoperasian dan pengurusan ICT MDKS dengan meminimumkan kerosakan atau kemusnahan;

b) Melindungi kepentingan pihak-pihak yang bergantung kepada ICT MDKS dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

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. Terdapat empat (4) komponen asas keselamatan ICT iaitu :-

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna;
d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKICT MDKS merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :-

a) **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) **Integriti** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c) **Tidak Boleh Disangka** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d) **Kesahihan** - Data dan maklumat hendaklah dijamin kesahihannya; dan
e) **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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.

SKOP

Sistem ICT MDKS terdiri daripada manusia, perkakasan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT MDKS menetapkan keperluan-keperluan asas berikut :-

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Sistem ICT MDKS terjamin keselamatannya sepanjang masa, DKICT MDKS merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT MDKS. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara- perkara berikut :-

a) **Perkakasan**

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

b) **Perisian**

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

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.
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 agensi. Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat- maklumat arkib dan lain-lain

e) **Manusia**

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

Setiap perkara di atas perlu diberi perlindungan rapi.Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT MDKS dan perlu dipatuhi adalah seperti berikut :-

a) Akses atas dasar perlu mengetahui

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

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MDKS. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah :-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT MDKS 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

DKICT MDKS 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.

PERKARA 01 - DASAR KESELAMATAN ICT

OBJEKTIF		
DKICT MDKS diwujudkan untuk melindungi aset ICT MDKS bagi memastikan kelancaran operasi organisasi secara berterusan, meminimumkan kerosakan atau kemusnahan aset- aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.		
KENYATAAN DASAR		**TINDAKAN**
DM-010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Yang Dipertua (YDP) dibantu oleh CIO dan ICTSO yang dipengerusikan oleh Ketua Pegawai Maklumat (CIO) dengan keahlian terdiri daripada Pengurus ICT merangkap Pegawai Keselamatan ICT (ICTSO) serta semua CIO, Jabatan di bawahnya.	YDP
DM-010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna MDKS merangkumi semua warga MDKS, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan MDKS dan semua Jabatan/Agensi di bawahnya.	Semua ICTSO
DM-010103 Penyelenggaraan Dasar		
	DKICT MDKS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT MDKS :- a) Kenalpasti dan tentukan perubahan yang diperlukan;	ICTSO

	b) Kemukakan cadangan pindaan secara bertulis untuk pembentangan dan persetujuan Jawatan Kuasa Pemandu ICT (JPICT) atau yang setaraf dengannya yang di pengerusikan oleh Yang Dipertua; c) Perubahan yang telah dipersetujui oleh JPICT mestilah dimaklumkan kepada semua pengguna; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau sekiranya terdapat sebarang keperluan penambahbaikan dan arahan Kerajaan dari semasa ke semasa.	
DM-010104 Pemakaian Dasar		
	DKICT MDKS adalah terpakai kepada semua pengguna ICT MDKS dan tiada pengecualian diberikan.	Semua Pengguna

PERKARA 02 : ORGANISASI KESELAMATAN

OBJEKTIF	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT MDKS	
KENYATAAN DASAR	**TINDAKAN**
Infrastruktur Organisasi Keselamatan	
DM-020101 Yang Dipertua	
Peranan dan tanggungjawab YDP adalah seperti berikut :- a) Membaca, memahami dan mematuhi DKICT MDKS; b) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT MDKS; c) Memastikan semua pengguna mematuhi DKICT MDKS; d) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MDKS. Dan f) Menandatangani SURAT PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KUALA SELANGOR. (Lampiran A)	YDP

DM-020102 Ketua Pegawai Maklumat (CIO)		
	Ketua Pegawai Maklumat (CIO) adalah Setiausaha MDKS atau pegawai yang telah dilantik oleh MDKS. Peranan dan tanggung jawab CIO adalah seperti berikut :- a) Membaca, memahami dan mematuhi DKICT MDKS; b) Membantu dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT MDKS; c) Menentukan keperluan keselamatan ICT MDKS; dan .	CIO
DM-020103 Pengurus ICT		
	Pengurus ICT ialah Pegawai Teknologi Maklumat MDKS. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut :- a) Membaca, memahami dan mematuhi DKICT MDKS; b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MDKS; c) Menentukan kawalan akses semua pengguna terhadap aset ICT MDKS; d) Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MDKS; dan	ICTSO

	e) Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KUALA SELANGOR. (Lampiran A). Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau sekiranya terdapat sebarang keperluan penambahbaikan dan arahan Kerajaan dari semasa ke semasa.	
DM-020104 Pegawai Keselamatan ICT (ICTSO)		
	ICTSO MDKS adalah Penolong Pegawai Teknologi Maklumat MDKS. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :- a) Membaca, memahami dan mematuhi DKICT MDKS; b) Mengurus keseluruhan program-program keselamatan ICT MDKS; c) Menguatkuasakan DKICT MDKS; d) Memberi penerangan, taklimat dan pendedahan berkenaan DKICT MDKS kepada semua pengguna MDKS; e) Mewujudkankan melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT MDKS; f) Menjalankan pengurusan risiko; g) Menjalankan audit, mengkaji semula, h) Melaporkan insiden keselamatan ICT kepada Ketua Jabatan (Pegawai Insiden Keselamatan ICT dan memaklumkan kepada CIO.	ICTSO

	i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT & memperakukan langkah-langkah baik pulih dengan segera; j) Melaporkan sebarang salah laku pengguna yang melanggar DKICT MDKS kepada CIO; k) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT MDKS; l) Menyedia, melaksanakan & menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; m) Menyedia dan melaksanakan menyelaras penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MDKS; dan n) Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KUALA SELANGOR. (Lampiran A)	
DM-020105 Pentadbir Sistem ICT		
	Pentadbir Sistem ICT ialah Penolong Pegawai Teknologi Maklumat MDKS dan semua Ketua Jabatan merupakan Pentadbir Sistem ICT di Jabatan masing-masing. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :-	PPTM MDKS, Pegawai yang diturunkan kuasa

	a) Membaca, memahami dan mematuhi DKICT MDKS. b) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT MDKS; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Melaporkan sebarang insiden keselamatan ICT kepada ICTSO masing-masing; f) Menyimpan dan menganalisis rekod jejak audit;	
DM-020106 Pengguna		
	Pengguna adalah semua warga MDKS, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan MDKS dan Jabatan/Agensi di bawahnya. Peranan dan tanggungjawab pengguna adalah seperti berikut :-	Pengguna

a) Membaca, memahami dan mematuhi DKICT MDKS;

b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;

c) Lulus tapisan keselamatan (jika berkaitan);

d) Melaksanakan prinsip DKICT MDKS dan menjaga kerahsiaan maklumat MDKS;

e) Melaksanakan langkah - langkah perlindungan seperti berikut :-

- Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
- Menentukan maklumat sedia untuk digunakan;
- Menjaga kerahsiaan kata laluan;
- Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan,pemprosesan, penyimpanan penghantaran penyampaian, pertukaran dan pemusnahan; dan
- Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

f) Melaporkan segera sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO;

	g) Menghadiri program-program kesedaran mengenai keselamatan ICT MDKS; dan h) Menandatangani borang / surat AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KUALA SELANGOR. (Lampiran A)	
DM-020107	**Pasukan Pengendali Insiden Keselamatan ICT MDKS (CERT MDKS)**	
	Keanggotaan CERT MDKS adalah seperti berikut :- **Pengarah CERT:** CIO MDKS (Setiausaha) **Pengurus CERT:** Pegawai Keselamatan ICT (ICTSO, MDKS) **Ahli :** • Ketua Jabatan MDKS • Pen. Pegawai Teknologi Maklumat MDKS • Juruteknik IT Peranan dan tanggungjawab CERT MDKS adalah seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT MDKS dan menilai tahap dan jenis insiden; b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindakbalas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya;	

	e) Memberi khidmat nasihat kepada semua CIO mengenai tindakan pemulihan dan pengukuhan; f) Menyebarkan makluman berkaitan pemulihan dan pengukuhan kepada semua pengguna MDKS; dan g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT MDKS yang digunakan oleh pihak ketiga.		
DM-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga		
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar / asing dikawal. Perkara yang perlu dipatuhi termasuk yang berikut :- a) Membaca, memahami dan mematuhi DKICT MDKS; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga dan akses kepada aset ICT MDKS perlu berlandaskan kepada perjanjian kontrak.	Semua CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

	Perkara- perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai :- • DKICT MDKS; • Tapisan Keselamatan; • Perakuan Akta Rahsia Rasmi 1972; • Hak Harta Intelek; dan • Arahan Teknologi Maklumat. e) Memastikan semua syarat keselamatan yang dinyatakan dengan jelas dalam perjanjian pihak ketiga. f) Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KUALA SELANGOR. (Lampiran A). g) Menandatangani *Non-Disclosure Agreement (NDA)* sebagaimana **Lampiran D.**	

PERKARA 03: PENGURUSAN ASET

Objektif		
Memberi dan menyokong perlindungan keselamatan yang bersesuaian ke atas semua aset ICT MDKS		
DM-030101 Inventori Aset		
	Semua aset ICT MDKS hendaklah direkodkan. Mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.	Pentadbir Sistem ICT dan Pegawai Aset
	Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah jagaan dan kawalannya.	Semua Pengguna
Pengelasan dan Pengendalian Maklumat		
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
DM-030201 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :- a) Rahsia besar b) Rahsia c) Sulit d) Terhad	Pegawai yang diberi kuasa
	Setiap pengguna adalah bertanggung jawab mengurus maklumat bersesuaian dengan peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan.	Semua pengguna

DM-030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut :- a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.;	Semua Pengguna

PERKARA 04: KESELAMATAN SUMBER MANUSIA

Objektif		
Memastikan semua sumber manusia yang terlibat termasuk warga MDKS, kontraktor, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT MDKS.		
Keselamatan ICT Dalam Tugas Harian		
DM-040101 Tanggungjawab Keselamatan		
	Peranandantanggung jawab pengguna terhadap keselamatan ICT MDKS mestilah lengkap, jelas, direkodkan, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.	Semua Pengguna
	Keselamatan ICT MDKS merangkumi tanggungjawab pengguna dalam menyediakan & memastikan ngan ke atas semua aset atau sumber ICT MDKS yang digunakan di dalam melaksanakan tugas harian.	
DM-040102 Terma dan Syarat Perkhidmatan		
	Semua pengguna MDKS yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa	Semua Pengguna MDKSyang dilantik
DM-040103 Perakuan Akta Rahsia Rasmi		
	Semua pengguna yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua Pengguna

DM-040104 Sebelum Berkhidmat		
	Semua pengguna mestilah memahami tanggungjawab masing-masing ke atas keselamatan aset ICT MDKS bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Peranan dan tanggung jawab penjawat awam,kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dengan aset ICT Kerajaan perlu dinyatakan dengan jelas dan terperinci sebelum, semasa dan selepas perkhidmatan; dan b) Penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Semua Pengguna
DM-040105 Dalam Perkhidmatan		
	Semua Pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT MDKS dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut :-	Semua Pengguna

	a) Memastikan semua pengguna MDKS menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh MDKS; b) Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT MDKS diberi kepada semua pengguna MDKS dan sekiranya perlu diberikan kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin ke atas semua pengguna MDKS, sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan dalam DKICT MDKS; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT MDKS. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada pihak ICT masing-masing	
DM-040106 Tamat Perkhidmatan Atau Bertukar		
	Memastikan semua pengguna MDKS diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari MDKS. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Memastikan semua aset ICT Kerajaan dikembalikan mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan	Semua Pengguna MDKS yang dilantik

	b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan / atau terma perkhidmatan.	

PERKARA 05: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif		
Melindungi pejabat dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
DM-050101 Perimeter Keselamatan Fizikal		
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut :- a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c) Memperkukuhkan dinding dan siling; d) Memasang alat penggera atau kamera; e) Mengehadkan jalan keluar masuk; f) Mengadakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan h) Mewujudkan perkhidmatan kawalan keselamatan.	Semua ICTSO, Ketua Pegawai Keselamatan yang dilantik (jika berkaitan)

DM-050102 Kawalan Masuk Fizikal		
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna MDKS hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat boleh mendapatPas keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c) Semua pas keselamatan hendaklah diserahkan balik kepada bahagian berkenaan apabila pengguna berhenti atau bersara; d) Setiap pelawat hendaklah mendaftar di pintu utama terlebih dahulu; e) Kehilangan pas mestilah dilaporkan dengan segera; f) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT MDKS	
DM-050103 Kawasan Larangan		
	Semua pengguna dilarang berada di Pusat Data (*Data Centre*) MDKS/Jabatan/Agensi kecuali dengan kebenaran dan/atau ditemani oleh pegawai yang diberi kuasa. Pusat Data merupakan kawasan larangan yang dihadkan kemasukannya bagi melindungi aset ICT MDKS yang terdapat di dalam kawasan tersebut.	

	Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
Keselamatan Peralatan		
Objektif : Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan.		
DM-050201 Peralatan ICT		
	Semua pengguna perlu mematuhi langkah-langkah keselamatan seperti berikut :- a) Menyemak dan memastikan semua perkakasan ICT dibawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c) Bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; d) Dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan; e) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; f) Memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan seperti *hard disk*, disket, *thumbdrive* dan *external hard disk*;	

	g) Melindungi semua peralatan sokongan ICT daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; h) Bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah jagaan dan / atau kawalannya; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; l) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; m) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pegawai Aset/ Pentadbir Sistem ICT MDKS;	

	o) Sebarang kerosakan perkakasan ICT MDKS hendaklah dilaporkan kepada Pentadbir Sistem ICT MDKS untuk di baik pulih; p) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT MDKS tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; q) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; r) Dilarang sama sekali mengubah password administrator yang telah ditetapkan oleh pihak ICT; s) Bertanggungjawab terhadap perkakasan, perisian dan maklumatdi bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t) Memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; dan u) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO MDKS/Jabatan/Agensi.	
DM-050202 Media Storan		
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, *external hard disk* dan media storan lain.	

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-

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

b) Bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;

c) Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;

d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;

e) Media storan & peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat.

f) Akses untuk memasuki penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;

g) Akses dan pergerakan kepada media storan perlu direkodkan;

h) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;

	i) Mengadakan salinan atau penduaan (data *backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	
DM-050203 Media Perisian dan Aplikasi		
	Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di Jabatan/Agensi; b) Sistem aplikasi dalaman tidak dibenarkan diagih / didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada media storan 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.	Semua Pengguna

DM-050204 Penyelenggaraan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; c) Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; d) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan e) Memaklumkan kepada pengguna sebelum penyelenggaraan dilakukan mengikut jadual yang ditetapkan atau atas keperluan.	
DM-050205 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat		
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-	

	a) Mendapatkan kelulusan Pegawai Aset / Pentadbir Sistem ICT Kementerian / Jabatan/ Agensi bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan.	
DM-050206 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar		
	Bagi peralatan yang dibawa masuk/keluar pejabat, langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT MDKS; b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh MDKS/Jabatan bagi membawa masuk/keluar peralatan (Lampiran C - Borang Pengisytiharan Barang Keluar/Masuk); dan c) Memastikan peralatan yang dibawa keluar tidak mengandungi maklumat Kerajaan.	Semua Pengguna
DM-050207 Pelupusan		
	Pelupusan melibatkan semua peralatan ICT MDKS yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori. Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MDKS.	

	Langkah - langkah seperti berikut hendaklah diambil :- a) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c) Media storan (*internal/external hard disk*) hendaklah dikeluarkan dan disimpan di tempat yang telah dikhaskan dengan ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d) Pegawai Aset bertanggungjawab merekodkan butir- butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset dan Stor (MyAsset); e) Pelupusan peralatan ICT MDKS hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; f) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut :- i. Menyimpan mana-mana peralatan ICT MDKS yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan dan menyimpan komponen dalaman CPU seperti RAM, *Hard disk*, *Motherboard* dan sebagainya;	

	ii. Menyimpan dan memindahkan perkakasan tambahan komputer seperti UPS, speaker atau mana-mana peralatan yang berkaitan ke mana-mana bahagian di Kementerian / Jabatan / Agensi; iii. Membawa keluar dari pejabat mana - mana peralatan ICT MDKS yang hendak dilupuskan;dan iv. Melupuskan sendiri peralatan ICT kerana kerja- kerja pelupusan di bawah tanggungjawab MDKS. g) Pengguna ICT MDKS bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin kepada media storan kedua seperti disket atau *thumbdrive* sebelum maklumat tersebut dihapuskan daripada peralatan komputer yang hendak dilupuskan.	
DM-050208 *Clear Desk* dan *Clear Screen*		
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk b*ermaksud tidak meninggalkan sebarang maklumat penting di atas meja apabila pengguna tidak berada di tempatnya. *Clear Screen* bermaksud tidak memaparkan sebarang maklumat penting di paparan skrin apabila pengguna tidak berada di tempatnya. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :-	

	a) Menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b) Maklumat-maklumat penting hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan c) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat atau media output yang lain.	
Keselamatan Persekitaran		
Objektif: Melindungi aset ICT MDKS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan		
DM-050301 Kawalan Persekitaran		
	Bagi mengelakkan kerosakan terhadap pejabat dan aset ICT MDKS, semua cadangan berkaitan pejabat sama ada urusan perolehan, penyewaan atau pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pegawai yang berkenaan. Bagi menjamin keselamatan persekitaran, langkah- langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat yang menempatkan pusat data, bilik percetakan, peralatan komputer dan sebagainya dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua Pengguna

	c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dilihat dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g) Semua peralatan perlindungan hendaklah diperiksa dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu	
DM-050302 Kabel		
	Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah- langkah keselamatan yang perlu diambil adalah seperti berikut :- a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada sebarang kerosakan; c) Memastikan laluan pemasangan kabel yang sesuai; d) Membuat pelabelan kabel.	ICTSO

DM-050303 Bekalan Kuasa		
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa :- a) Semua peralatan ICT MDKS hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti dibilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual	
DM-050304 Prosedur Kecemasan		
	Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a) Hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada 'Garis Panduan Keselamatan MDKS 2007'; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada pegawai yang berkenaan.	Semua Pengguna

Keselamatan Dokumen dan Sistem Dokumentasi		
DM-050401 Dokumen		
	Bagi memastikan integriti maklumat, semua pengguna perlu mengambil langkah-langkah berikut: a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c) Setiap dokumen hendaklah di fail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan; e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f) Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan g) Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua Pengguna

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif		
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
Pengurusan Prosedur Operasi		
DM-060101 Pengendalian Prosedur		
	Perkara yang perlu dipatuhi adalah seperti berikut :- a) Semua prosedur keselamatan ICT MDKS yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan - arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	ICTSO
DM-060102 Kawalan Perubahan		
	Perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengubahsuaian yang melibatkan perkakasan,sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai yang berkenaan atau pemilik aset ICT terlebih dahulu;	Semua Pengguna

	b) Aktiviti-aktiviti seperti memasang, menyenggara,menghapus & mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pegawai yang berkenaan dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
DM-060103 Pengasingan Tugas dan Tanggungjawab		
	Skop tugas dan tanggung jawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan 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.	Semua Pengurus ICT, ICTSO
Perancangan dan Penerimaan Sistem		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
DM-060201 Perancangan Kapasiti		
	Perkara yang perlu dipatuhi adalah seperti berikut:	

	a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT
DM-060202 Penerimaan Sistem		
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO dan Pentadbir Sistem ICT
Perisian Berbahaya		
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.		
DM-060301 Perlindungan dari Perisian Berbahaya		
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Prevention System* (IPS) dan mengikut prosedur penggunaan yang betul dan selamat;	Semua ICTSO dan Pentadbir Sistem ICT

	b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemas kini *pattern* anti virus dari semasa ke semasa; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana- mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian/aplikasi yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

Housekeeping		
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa boleh diakses.		
DM-060401 *Backup*		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; c) Menguji sistempenduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; dan e) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*.	

DM-060402 Sistem Log		
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO Kementerian/ Jabatan/ Agensi.	
Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
DM-060501 Kawalan Infrastruktur Rangkaian		
	Infrastruktur rangkaian mestilah di kawal dan diuruskan sebaik mungkin bagi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah - langkah yang perlu dipertimbangkan :- a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaia yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;	Semua Pentadbir Sistem ICT

	c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta di konfigurasi; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MDKS; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO Jabatan /Agensi; h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang bolehmengancam sistem dan maklumat MDKS; i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MDKS hendaklah mendapat kebenaran ICTSO; k) Semua pengguna hanya dibenarkan menggunakan rangkaian MDKS sahaja. Penggunaan modem dan rangkaian MDKS secara serentak adalah dilarang sama sekali;	

	l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan; dan; m) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
Pengurusan Media		
Objektif: Melindungi aset ICT MDKS dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.		
DM-060601 Penghantaran dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Sistem Kementerian /Jabatan /Agensi terlebih dahulu.	Semua Pengguna
DM-060602 Prosedur Pengendalian Media		
	Perkara yang perlu dipatuhi adalah seperti berikut :- a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat;	Semua Pentadbir Sistem ICT

	f) Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
DM-060603 Pengurusan Pertukaran Maklumat		
	Pengurusan pertukaran Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin. Langkah-langkah bagi Pengurusan Pertukaran Maklumat adalah seperti berikut :- a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MDKS dengan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripadacapaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MDKS; d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat MDKS.	Semua Pengguna

Keselamatan Komunikasi		
Objektif: Melindungi aset ICT MDKS melalui sistem komunikasi yang selamat.		
DM-060701	**Mel Elektronik (E-mel)**	
	Penggunaan e-mel MDKS hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam 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 yang perlu dipatuhi adalah seperti berikut :- a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MDKS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan; c) Setiap e-mel yang disediakan perlu mematuhi format yang telah ditetapkan oleh MDKS; d) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; e) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-melrasmi dan pastikan alamat e-mel penerima adalah betul;	Semua Pengguna

	f) Penggunaan fail kepilan (*attachment*) dibuat sekiranya perlu, tidak melebihi empat puluh (40) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; g) Penghantaran lampiran dalam format/*extension " *.exe, *.bat, *.hta, *.cmd* dan *.com"* tidak dibenarkan; h) Mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; i) Mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; j) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; k) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; l) Tentukan tarikh dan masa sistem komputer adalah tepat; m) Hanya warga MDKS sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi MDKS; n) Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; o) Bahagian Pentadbiran dan Pengurusan Sumber Manusia MDKS perlu memaklumkan sebarang status	

	pengguna (bertukar Jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke MDKS bagi tujuan pengemaskinian e-mel yang terlibat; dan p) Pengguna adalah mewakili diri sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik.	
DM-060702 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga		
	Memastikan pelaksanaan dan tahap penyenggaraan keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut :- a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak dan diaudit dari semasa ke semasa; dan c) Pengurusan kepada perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambahbaik polisi keselamatan, prosedur dan kawalan maklumat sedia ada,perlu mengambilkira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

DM-060703 Pemantauan		
	Bertujuan memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut :- a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam MDKS atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	

PERKARA 07 : KAWALAN CAPAIAN

Objektif		
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT MDKS.		
Dasar Kawalan Capaian		
DM-070101 Keperluan Dasar		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Semua Pentadbir Sistem ICT
Pengurusan Capaian Pengguna		
Objektif: Mengawal capaian pengguna ke atas aset ICT MDKS.		
DM-070201 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 sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan yang ditetapkan.	

	d) Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f) Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Pengguna bercuti panjang; ii) Bertukar bidang tugas kerja; ii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan.	
DM-070202 Hak Capaian		
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua Pentadbir Sistem ICT
DM-070203 Pengurusan 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 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 di kompromi;	Semua Pengguna

	c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) manakala kata laluan bagi pembangunan aplikasi sistem yang baru mestilah sekurang-kurangnya dua belas (12) aksara dengan kombinasi aksara, angka dan aksara khas berkuat kuasa Januari 2008; d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan w*indows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan.	

DM-070204 Kad Pintar		
	a) Penggunaan kad pintar Kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan elektronik yang dikhususkan. b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d) Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak ICT masing-masing.	Semua Pengguna MDKS yang terlibat
Kawalan Capaian		
Objektif: Menghalang capaian yang tidak sah dan tanpa kebenaran serta boleh menyebabkan kerosakan		
DM-070301 Kawalan Capaian Rangkaian		
	Perkara yang perlu dipatuhi adalah seperti berikut:- a) Memastikan pengguna membuat capaian pada sistem yang dibenarkan sahaja; b) Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan	Semua Pentadbir Sistem ICT

	d) Mewujud dan melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan rangkaian boleh diakses oleh pengguna.	
DM-070302 Capaian Jarak Jauh		
	a) Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah ***Remote Access*** mestilah menggunakan kaedah penyulitan (*encryption*); b) Lokasi bagi akses ke sistem ICT MDKS hendaklah dipastikan selamat; c) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	
DM-070303 Capaian Internet		
	a) Penggunaan Internet hendaklah dipantausecara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnyake dalam rangkaian MDKS. b) PenggunaanInternet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pentadbir Sistem ICT Semua Pengguna

	d) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; e) Penggunaan modem telefon untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; f) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :- i. Memuat naik, memuat turun, menyimpan dan menggunakan sebarang aplikasi seperti permainan elektronik, video / audio, lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan yang mengandungi unsur-unsur lucah. g. Pengguna hendaklah berhenti dan memutuskan talian dengan serta merta sekiranya menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan.	
Kawalan Capaian Sistem dan Aplikasi		
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		

DM-070401 Capaian Sistem Pengoperasian		
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Merekodkan capaian yang berjaya dan gagal; dan c) Membekalkan kemudahan untuk pengesahan; bagi sistem kata kunci digunakan, kualiti kata kunci perlu mendapat pengesahan. Kaedah - kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut :- a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d) Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi termasuk berikut :-	Semua Pentadbir Sistem ICT, ICTSO

	a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; d) Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan e) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
DM-070402 Sistem Maklumat dan Aplikasi		
	Capaian sistem dan aplikasi di MDKS adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a) Penggunahanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	

	c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e) Memastikan kawalan sistem adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
Audit		
DM-070501 Pengauditan dan Forensik ICT		
	ICTSO mestilah bertanggungjawab merekod dan menganalisa: a) Sebarang percubaan pencerobohan kepada sistem ICT MDKS; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam* , pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*);	Semua ICTSO

	c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan- bahan lucah, berunsur fitnah dan propaganda anti Kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem. Langkah-langkah yang perlu diambil adalah seperti berikut :- a) ICTSO akan menentukan prosedur pengumpulan bahan bukti (*hard disk*/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b) Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c) Sekiranya hasilsiasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan. Semua proses dan hasil siasatan adalah SULIT.	

DM-070502 Jejak Audit		
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi :- a) Maklumat identity pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; c) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; d) Catatan jejak audit dari semasa ke semasa untuk membantu mengesan aktiviti yang tidak normal dengan lebih awal; e) Menyediakan laporan jika perlu; f) Aktiviti perlindungan dari kerosakan, kehilangan, penghapusan, pemalsuan pengubahsuaian yang tidak dibenarkan.	

PERKARA 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif		
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
DM-080101 Keperluan Keselamatan		
	Perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan c) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhikeperluan keselamatan yang telah ditetapkan sebelum digunakan	

DM-080102 Pengesahan Data Input		
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Semua Pentadbir Sistem ICT
DM-080103 Kawalan Prosesan		
	Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Semua Pentadbir Sistem ICT
DM-080104 Pengesahan Data Output		
	Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Semua Pentadbir Sistem ICT
Kriptografi		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
DM-080201 Penyulitan		
	Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua Pengguna
DM-080202 Pengurusan Infrastruktur Kunci Awam (PKI)		
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua Pengguna
Fail Sistem		
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		

DM-080301 Kawalan Fail Sistem		
	Perkara yang perlu dipatuhi adalah seperti berikut :- a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Semua Pentadbir Sistem ICT
Pembangunan dan Sokongan Sistem		
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
DM-080401 Kawalan Perubahan		
	Perubahan atau pengubahsuaian keatas sistem maklumat dan aplikasihendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Semua Pentadbir Sistem ICT

DM-080402 Pembangunan Secara *Outsource*		
	Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh Bahagian Teknologi Maklumat MDKS. *Source code* adalah menjadi hak milik MDKS.	Semua Pentadbir Sistem ICT
DM-080403 Kawalan dari Ancaman Teknikal		
	Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenal pasti tahap risiko yang bakal dihadapi.	Semua Pentadbir Sistem ICT

PERKARA 09: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Objektif		
Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT MDKS dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej MDKS dan sistem penyampaian perkhidmatan.		
Pengurusan Insiden Keselamatan ICT		
DM-090101 Mekanisme Pelaporan Insiden Keselamatan ICT		
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada CERT MDKS dengan kadar segera :- a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian system yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlakupercubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut :-	Semua Pengguna CERT MDKS Semua Pengguna

	i. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada CERT MDKS untuk pengendalian dan pengumpulan statistic insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. **ii. CERT MDKS** Pasukan CERT MDKS akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada Sebagai *input* atau untuk tindakan seterusnya. **iii. Tanggungjawab Pengguna** Semua pengguna yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO, kerentanan (*vulnerabality*) yang diperhatikan atau disyaki terdapat dalam system maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti cubaan menceroboh. **iv. Tindakan Dalam Keadaan Berisiko Tinggi** Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan	Semua CIO, ICTSO

	serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak	
DM-090102 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT		
	Semua pegawai pasukan pengendali insiden keselamatan ICT atau CERT MDKS perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan CERT MDKS dan GCERT MAMPU. CERT MDKS menerima aduan atau laporan daripada pengguna atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguat kuasa undang-undang. CERT MDKS yang diketuai oleh Pengurus ICT akan menjalankan tindakan pengendalian secara capaian jarak jauh (*remote*) atau *on-site.* Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan perlu dihantar bagi mendapatkan maklum balas GCERT MAMPU. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan perlu dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT MDKS	

	seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan / *Business Resumption Plan* (*BRP*) perlu diaktifkan atau sebaliknya. Pengesahan perlu dihantar kepada CIO bagi mengaktifkan *BRP*. Laporan insiden yang tidak memerlukan *BRP* akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di Lampiran B.	
DM-090103 Pengurusan Maklumat Insiden Keselamatan ICT		
	Perkara yang perlu dipatuhi adalah seperti berikut :- a) Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar- dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MDKS; b) Memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan.	

	Penyediaan bahan-bahan bukti seperti jejak audit, backup secara berkala dan media backup offline hendaklah mengikut amalan terbaik yang disarankan oleh Kerajaan dari semasa ke semasa; c) Memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan; dan d) Perkara-perkara yang mesti dipatuhi termasuk yang berikut :- i. Melindungi Integriti semua bahan bukti; ii. Menyalin bahan bukti oleh personel yang dipertanggung jawabkan; iii. Merekodkan semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan tools yang digunakan; iv. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan v. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang perlukan.	

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif		
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
Dasar Kesinambungan Perkhidmatan		
DM-100101Pelan Kesinambungan Perkhidmatan		
	Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada roses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian :- a) Mengenalpasti tanggungjawab dan prosedur kecemasan atau pemulihan. b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan e) Membuat penduaan; dan	

	f) Menguji dan mengemaskini pelan sekurang - kurangnya setahun sekali	
DM-100102 Pengurusan Kesinambungan Perkhidmatan		
	Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej MDKS terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MDKS di samping menyediakan pelan tindakan bagi mewujudkan ketahanandan keupayaan bertindak yang berkesan. Pengurus ICT adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT MDKS.	Semua ICTSO

PERKARA 11 : PEMATUHAN

Objektif		
Meningkatkan tahap keselamatan ICTbagi mengelak dari pelanggaran kepada DKICT MDKS.		
Pematuhan dan Keperluan Perundangan		
DM-110101 Pematuhan Dasar		
	DKICT MDKS dan undang-undang atau peraturan - peraturan lain yang berkaitan yang berkuat kuasa hendaklah dibaca, difahami dan dipatuhi. Semua aset ICT MDKS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan KetuaJabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua Pengguna
DM-110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal		
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan.	ICTSO
DM-110103 Pematuhan Keperluan Audit		
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	Semua Pengguna

	Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
DM-110104 Keperluan Perundangan		
	Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi: a) Arahan Keselamatan; b) *"Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)"; c) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan". d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)" e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f) Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam"; g) Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";	Semua Pengguna

	h) Surat Pekeliling Perbendaharaan Bilangan 8 Tahun 2006 bertajuk "Peraturan Perolehan Perkhidmatan Perunding"; i) Pekeliling Am Bilangan 1 Tahun 2006 bertajuk "Pengurusan laman Web/Portal Sektor Awam"; j) Surat Arahan MAMPU bertajuk "Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 1 Jun 2007; k) Surat Arahan MAMPU bertajuk "Langkah-langkah Pemantapan Pelaksanaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 23 November 2007; l) Surat Arahan Ketua Setiausaha Negara dengan rujukan UPTM(S)159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan" bertarikh 20 Oktober 2006; m) Akta Rahsia Rasmi 1972; n) Akta Tandatangan Digital 1997; o) Akta Jenayah Komputer 1997; p) Akta Hak cipta (Pindaan) Tahun 1997; q) Akta Komunikasi dan Multimedia 1998 r) Arahan Teknologi Maklumat 2007; s) Perintah-Perintah Am; dan t.Arahan Perbendaharaan.	

Tindakan Tatatertib		
Objektif : Meningkatkan kesedaran dan pematuhan ke atas DKICT MDKS.		
DM-110201 Pelanggaran Dasar / Perundangan		
	Pelanggaran DKICT MDKS dan semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara terperingkat di bawah Akta Rahsia Rasmi 1972 akan dikenakan tindakan tatatertib.	Semua Pengguna

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CERT MDKS	Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
DKICT MDKS	Dasar Keselamatan ICT MDKS dan semua Jabatan/Agensi di bawahnya.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan(*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Pengendali Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology*. (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Prevention System(IPS)	Sistem Pencegah Pencerobohan Perkakasankeselamatan komputer yang memantau rangkaiandan/atau aktiviti yang berlaku dalam sistem bagi