DASAR KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

DKICT

ARKIB NEGARA MALAYSIA

Versi 1.0
2 Mei 2014

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT Arkib Negara Malaysia (DKICT ANM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) ANM. Dasar ini juga menerangkan kepada semua pengguna di ANM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT ANM.

OBJEKTIF

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

Objektif utama DKICT ANM ialah seperti berikut :-

a. Memastikan kelancaran pengoperasian dan pengurusan ICT ANM dengan meminimumkan kerosakan atau kemusnahan;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada ICT ANM daripada 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; dan
d. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

DKICT ANM 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 Disangkal — 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 ANM terdiri daripada manusia, perkakasan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT ANM 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 ANM terjamin keselamatannya sepanjang masa, DKICT ANM 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 ANM. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :-

a. Perkakasan
   Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. 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 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 ANM dan perlu dipatuhi adalah seperti berikut :-

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT ANM 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 ANM. 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 ANM 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 ANM 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 ANM diwujudkan untuk melindungi aset ICT ANM 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.		
DK0101 Dasar Keselamatan ICT		
DK010101	Pelaksanaan Dasar	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah (KP) dibantu dan dipengerusikan oleh Ketua Pegawai Maklumat (CIO) dengan keahlian terdiri daripada Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat dan Juruteknik Komputer.	KP ANM
DK010102	Penyebaran Dasar	
	Dasar ini perlu disebarkan kepada semua pengguna ANM merangkumi semua warga ANM, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan ANM.	ICTSO
DK010103	Penyelenggaraan Dasar	
	DKICT ANM 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 ANM :- a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemukakan cadangan pindaan secara bertulis untuk	ICTSO

	pembentangan dan persetujuan Jawatan Kuasa Pemandu ICT (JPICT) ANM yang di pengerusikan oleh KP ANM; c. Perubahan yang telah dipersetujui oleh JPICT mestilah dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	
DK010104	Pemakaian Dasar	
	DKICT ANM adalah terpakai kepada semua pengguna ICT ANM dan tiada pengecualian diberikan.	Pengguna

PERKARA 02 ORGANISASI KESELAMATAN

Objektif		
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT ANM.		
DK0201 Infrastruktur Organisasi Keselamatan		
DK020101	Ketua Pengarah	
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut :- a. Memastikan DKICT ANM dilaksanakan sepenuhnya di Arkib Negara Malaysia; b. Memastikan semua pengguna membaca, memahami dan mematuhi peruntukan-peruntukan di bawah DKICT ANM; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT ANM; dan e. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	KP ANM
DK020102	Ketua Pegawai Maklumat (CIO)	
	Ketua Pegawai Maklumat (CIO) adalah Timbalan Ketua Pengarah (TKP) Penyelidikan dan Pengembangan. Peranan dan tanggung jawab CIO adalah seperti berikut :-	CIO

	a. Membaca, memahami dan mematuhi DKICT ANM; b. Membantu KP ANM dalam memastikan DKICT ANM dilaksanakan sepenuhnya; c. Membantu KP ANM dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT ANM; d. Menilai dan mengkaji keberkesanan DKICT ANM; e. Menilai dan menentukan keperluan keselamatan ICT ANM; dan f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	
DK020103	Pengurus ICT	
	Pengurus ICT ialah Ketua Seksyen Teknologi Maklumat (STM). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut :- a. Membaca, memahami dan mematuhi DKICT ANM; b. Menguatkuasakan pelaksanaan DKICT ANM; c. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan ANM; d. Menentukan kawalan akses semua pengguna terhadap aset ICT ANM; e. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; f. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT ANM; dan	Pengurus ICT

	g. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	
DK020104	Pegawai Keselamatan ICT (ICTSO)	
	ICTSO adalah Ketua Seksyen Teknologi Maklumat (STM). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :- a. Membaca, memahami dan mematuhi DKICT ANM; b. Mengurus keseluruhan program-program keselamatan ICT ANM; c. Memberi penerangan, taklimat dan pendedahan berkenaan DKICT ANM kepada semua pengguna ANM; d. Mewujudkan dan melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT ANM; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Jabatan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Pengendali Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO;	ICTSO

	i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. Melaporkan sebarang salah laku pengguna yang melanggar DKICT ANM kepada CIO; k. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT ANM; l. Menyedia, melaksanakan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; m. Menyedia, melaksanakan dan menyelaras penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT ANM; dan n. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	
DK020105	Pentadbir Sistem ICT	
	Pentadbir Sistem ICT ialah Pegawai Teknologi Maklumat (PTM), Penolong Pegawai Teknologi Maklumat (PPTM) dan Juruteknik Komputer (JTK). Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :- a. Membaca, memahami dan mematuhi DKICT ANM; b. Pentadbir Sistem ICT terdiri daripada : i. Pentadbir Rangkaian dan Keselamatan; ii. Pentadbir Pangkalan Data; iii. Pentadbir Laman Web (*Webmaster*);	Semua PTM, PPTM, JTK ANM, Pegawai yang diturunkan kuasa

	iv. Pentadbir Pusat Data; v. Pentadbir Sistem Aplikasi; vi. Pentadbir E-mel; dan vii. Pentadbir Aset ICT. c. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	
DK02010501	Pentadbir Rangkaian dan Keselamatan	
	Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut :- a. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di ANM beroperasi sepanjang masa; b. Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna; c. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian ANM secara tidak sah seperti melalui peralatan modem dan *dial-up*; g. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan	Pentadbir Rangkaian dan Keselamatan

	h. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment*, SPA) serta penilaian risiko keselamatan maklumat.	
DK02010502	Pentadbir Pangkalan Data	
	Peranan dan tanggungjawab Pentadbir Pangkalan Data dan Keselamatan adalah seperti berikut :- a. Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b. Memastikan pangkalan data boleh digunakan pada setiap masa; c. Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; d. Melaksanakan proses *backup* dan *restoration* ke atas pangkalan data; e. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; f. Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; g. Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan h. Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data
DK02010503	Pentadbir Laman Web (*Webmaster*)	
	Peranan dan tanggungjawab Pentadbir Laman Web (*Webmaster*) adalah seperti berikut :-	Pentadbir Laman Web

	a. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan pengujian prestasi untuk memastikan akses yang lancar; c. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d. Menghadkan capaian Pentadbir Laman Web seksyen ke *web server*; e. Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal ANM; f. Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; g. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; h. Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; i. Melaksanakan proses *backup* dan *restoration* secara berkala; dan j. Melaporkan sebarang pelanggaran keselamatan portal/ laman web kepada ICTSO.	(*Webmaster*)
DK02010504	Pentadbir Pusat Data	
	Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut :-	Pentadbir Pusat Data

	a. Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b. Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c. Menjadualkan proses salinan (*backup and restore*) ke atas data dan sistem secara berkala; d. Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam DKICT; e. Melaksanakan prinsip-prinsip DKICT; dan f. Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	
DK02010505	Pentadbir Sistem Aplikasi	
	Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut :- a. Mengkaji cadangan pembangunan/ penyelarasan sistem/ modul di ANM; b. Membuat kajian semula serta memperbaiki sistem/ modul sedia ada di ANM; c. Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem/ modul di ANM; d. Membuat pemantauan dan penyelenggaraan terhadap sistem/ modul dari semasa ke semasa; e. Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem/ modul; f. Menyediakan dokumentasi sistem/ modul dan manual	Pentadbir Sistem Aplikasi

	pengguna; g. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; h. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; i. Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggodam; j. Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam mewujudkan akaun pengguna ke atas setiap sistem aplikasi; k. Memastikan salinan pendua (*backup*) sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual; l. Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan daripada penyalahgunaannya; dan m. Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi.	
DK02010506	Pentadbir E-mel	
	Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut :- a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;	Pentadbir E-mel

	b. Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel tertakluk kepada kemampuan ruang storan; d. Melaksanakan jadual *backup* dan pengarkiban emel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; e. Memastikan akaun e-mel pengguna sentiasa di dalam keadaan baik dan berfungsi; f. Melaksanakan aktiviti *housekeeping* terhadap akaun e-mel pengguna secara berkala; g. Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam; h. Memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan seperti serangan virus, serangan *e-mail spamming, phishing,* pencerobohan e-mel dan penyalahgunaan e-mel. Pentadbir e-mel hendaklah mengurus dan menangani insiden yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih; i. Melaksanakan penyelenggaraan ke atas aplikasi e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; j. Memantau status storan e-mel Pengurusan Atasan ANM dua (2) kali sehari dan memastikan e-mel Pengurusan Atasan ANM sentiasa tersedia untuk transaksi e-mel;	

	k. Memastikan semua peralatan aplikasi e-mel ANM sentiasa aktif; l. Menyediakan ruang *mailbox* yang mencukupi sekurang-kurangnya 500MB untuk setiap akaun emel dan jumlah ini adalah bergantung kepada keperluan pemilik akaun e-mel; m. Menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat-turun fail dengan memaklumkan lokasi *universal resource location* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan; n. Memastikan perjanjian penyelenggaraan sistem emel pada tahap premium (*premium service*) dengan pembekal-pembekal yang berkelayakan; o. Memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk server atau aplikasi dalaman ANM sahaja bagi tujuan keselamatan; p. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih; dan q. Memastikan pengguna e-mel ANM berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel ANM dan Internet ANM serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan.	
DK02010507	Pentadbir Aset ICT	
	Peranan dan tanggungjawab Pentadbir Aset ICT adalah seperti berikut :- a. Menguruskan aset-aset ICT ANM berdasarkan Tatacara	Pentadbir Aset ICT

	Pengurusan Aset Alih Kerajaan Malaysia; b. Merancang keperluan peralatan ICT ANM dan menyediakan spesifikasi teknikal yang bersesuaian; c. Memastikan semua aset ICT ANM yang baru diperoleh didaftarkan dalam Sistem Pengurusan Aset; d. Mengemaskini maklumat aset ICT dalam Sistem Pengurusan Aset berdasarkan maklumat semasa; e. Menyediakan ruang simpanan sementara yang selamat bagi peralatan ICT yang baru diterima oleh pihak pembekal; f. Memastikan keselamatan stor ICT sentiasa terjamin; g. Bertanggungjawab memantau setiap perkakasan ICT ANM yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; h. Melaksanakan inspektorat untuk memastikan peralatan dan perisian beroperasi dengan baik; i. Menyelaras dan memastikan kerja-kerja penyelenggaraan oleh pembekal dijalankan mengikut jadual yang telah ditetapkan; j. Menyelaras dan menguruskan penghantaran peralatan ICT untuk diselenggara dan dibaiki oleh pembekal sekiranya tidak boleh dilaksanakan dipihak STM sehingga selesai; k. Menjalankan pengujian peralatan ICT yang diterima selepas pelaksanaan penyelenggaraan oleh pihak pembekal; l. Mengambil tindakan yang bersesuaian dengan segera	

	apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; dan m. Menyimpan peralatan ICT yang dipulangkan ke tempat yang selamat.	
DK020106	Pengguna	
	Pengguna adalah semua Warga ANM, pembekal, pakar runding dan lain-lain yang bertugas dan/ atau berurusan dengan ANM. Peranan dan tanggungjawab pengguna adalah seperti berikut :- a. Membaca, memahami dan mematuhi DKICT ANM; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Lulus tapisan keselamatan (jika berkaitan); d. Melaksanakan prinsip-prinsip DKICT ANM dan menjaga kerahsiaan maklumat ANM; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia 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,	Pengguna

	penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. 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 ANM; dan h. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A).	
DK020107	Jawatankuasa Pemandu ICT (JPICT) ANM	
	Keanggotaan JPICT adalah seperti berikut : Pengerusi : Ketua Pengarah ANM Ahli : • Timbalan Ketua Pengarah (Penyelidikan dan Pengembangan)/ CIO • Timbalan Ketua Pengarah (Perancangan dan Pengurusan)/ CIO • Pengarah Bahagian Khidmat Pengurusan • Pengarah Bahagian Perancangan dan Penyelarasan • Pengarah Bahagian Rekod Kerajaan • Pengarah Bahagian Pengurusan Arkib • Pengarah Bahagian Pengembangan • Pengarah Bahagian Pengurusan, Penyelidikan dan Dokumentasi • Pengarah Bahagian Arkib Negarawan • Ketua Seksyen Pentadbiran dan Kewangan • Ketua Seksyen Teknologi Maklumat/ Pengurus ICT/ ICTSO	KP ANM

	Ahli-ahli Jemputan (bila perlu) : Ketua Seksyen Urus Setia : Seksyen Teknologi Maklumat Bidang kuasa : a. Menetapkan hala tuju dan strategi ICT ANM; b. Merancang, menyelaras dan memantau pelaksanaan program/ projek ICT ANM; c. Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Teknologi Maklumat (PSTM) ANM; d. Meluluskan projek-projek ICT ANM; e. Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; f. Merancang dan menentukan langkah-langkah keselamatan ICT; g. Melulus dan memperakukan perolehan ICT ANM untuk kelulusan JPICT Kementerian dan Jawatankuasa Teknikal ICT (JTICT) MAMPU berdasarkan Tatacara Perolehan ICT (SPA Bil. 2 Tahun 2009); h. Mengemukakan laporan kemajuan projek kepada JTICT MAMPU bagi projek ICT yang telah diluluskan; dan i. Menetapkan dan meluluskan dasar dan prosedur ICT ANM.	
DK020108	Pasukan Pemulihan Bencana / *Disaster Recovery Team* (DRT) ICT ANM	

	Keanggotaan DRT ICT adalah seperti berikut : Pengerusi : Pengurus ICT/ ICTSO Ahli : • Pegawai Teknologi Maklumat • Penolong Pegawai Teknologi Maklumat • Juruteknik Komputer Urus Setia : Seksyen Teknologi Maklumat Bidang kuasa : a. Membangunkan Dokumen Pelan Pemulihan Bencana (DRP) ICT; b. Menyediakan kemudahan pemulihan bencana atau Pusat Pemulihan Bencana (*Disaster Recovery Centre*, DRC); c. Membuat penilaian ke atas masalah dan jangkaan akibat bencana; d. Memaklumkan kepada Pengurusan Atasan berkenaan bencana, kemajuan pemulihan bencana dan masalah yang dihadapi; e. Mengaktifkan prosedur pemulihan bencana; f. Mengkoordinasi operasi pemulihan; g. Memantau operasi pemulihan dan memastikan jadual pemulihan dipatuhi; h. Mendokumentasikan operasi pemulihan; dan i. Mengkoordinasi simulasi pemulihan bencana.	DRT ICT

DK0202 Pihak Ketiga		
Objektif : Menjamin keselamatan semua aset ICT ANM yang digunakan oleh pihak ketiga.		
DK020201	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 ANM; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti 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 ANM perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai :- i. DKICT ANM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; dan v. Arahan Teknologi Maklumat. e. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT ARKIB NEGARA MALAYSIA. (Lampiran A) f. Pihak ketiga (pembekal, kontraktor, perunding dan	Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

	sebagainya) juga perlu menandatangani Borang Perakuan Untuk Ditandatangani Oleh Kontraktor Yang Terlibat Dengan Projek Kerajaan Menurut Akta Rahsia Rasmi 1972/ Declaration To Be Signed By Contractors, Official Secrets Act (OSA) 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperolehi sepanjang berkhidmat dengan ANM seperti di Lampiran B.	

PERKARA 03 PENGURUSAN ASET

Objektif		
Memberi dan menyokong perlindungan keselamatan yang bersesuaian ke atas semua aset ICT ANM.		
DK0301 Pengurusan Aset		
DK030101	Inventori Aset	
	Semua aset ICT ANM hendaklah direkodkan. Mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.	Pentadbir Aset ICT dan Pegawai Aset
	Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah jagaan dan kawalannya.	Pengguna
DK0302 Pengelasan dan Pengendalian Maklumat		
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
DK030201	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; atau 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.	Pengguna

DK030202	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; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT ANM dari diketahui umum.	Pengguna

PERKARA 04 KESELAMATAN SUMBER MANUSIA

Objektif		
Memastikan semua sumber manusia yang terlibat termasuk warga ANM, kontraktor, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT ANM.		
DK0401 Keselamatan ICT Dalam Tugas Harian		
DK040101	Tanggungjawab Keselamatan	
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT ANM mestilah lengkap, jelas, direkodkan, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT ANM merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT ANM yang digunakan di dalam melaksanakan tugas harian.	Pengguna
DK040102	Terma dan Syarat Perkhidmatan	
	Semua pengguna ANM yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Pengguna ANM yang dilantik
DK040103	Perakuan Akta Rahsia Rasmi	
	Semua pengguna yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Pengguna
DK040104	Sebelum Perkhidmatan	
	Semua pengguna mestilah memahami tanggungjawab masing-masing ke atas keselamatan aset ICT ANM bagi meminimumkan risiko seperti kesilapan, kecuaian,	Pengguna

	kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Peranan dan tanggungjawab 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.	
DK040105	Semasa Perkhidmatan	
	Semua Pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT ANM dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua pengguna ANM menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh ANM; b. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT ANM diberi kepada semua pengguna ANM dan sekiranya perlu diberikan kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa;	Pengguna ICTSO

	c. Memastikan adanya proses tindakan disiplin ke atas semua pengguna ANM, sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan dalam DKICT ANM; 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 ANM. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada pihak ICT masing-masing.	Pengguna
DK040106	Tamat Perkhidmatan Atau Bertukar	
	Memastikan semua pengguna ANM diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari ANM. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua aset ICT Kerajaan dikembalikan mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/ atau terma perkhidmatan.	Pengguna ANM yang dilantik

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif		
Melindungi pejabat dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
DK0501 Keselamatan Kawasan		
DK050101	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. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	Pengurus ICT, ICTSO, Ketua Pegawai Keselamatan yang dilantik (jika berkaitan)
DK050102	Kawalan Masuk Fizikal	
	Perkara yang perlu dipatuhi adalah seperti berikut :-	Pengguna dan

	a. Setiap pengguna ANM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat perlu mendaftar bagi mendapatkan Pas Keselamatan Pelawat di pintu masuk utama dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada Seksyen Pentadbiran dan Kewangan apabila pengguna berhenti atau bersara; d. Kehilangan pas mestilah dilaporkan dengan segera; dan e. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT ANM.	Pelawat
DK050103	Kawasan Larangan	
	Semua pengguna dilarang berada di Pusat Data (*Data Centre*) ANM kecuali dengan kebenaran dan/atau ditemani oleh pegawai yang diberi kuasa. Pusat Data merupakan kawasan larangan yang dihadkan kemasukannya bagi melindungi aset ICT ANM yang terdapat di dalam kawasan tersebut. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Pengguna
DK0502 Keselamatan Peralatan		
Objektif : Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan.		
DK050201	Peralatan ICT	
	Semua pengguna perlu mematuhi langkah-langkah keselamatan seperti berikut :-	Pentadbir Sistem ICT,

	a. Menyemak dan memastikan semua perkakasan ICT di bawah 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, 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	Pengguna

	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 hendak dibawa keluar dari premis ANM, perlulah mendapat kelulusan/ pengesahan Pegawai Aset Seksyen/ Negeri atau Pentadbir Sistem ICT ANM bagi tujuan pemantauan; m. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; n. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pegawai Aset/ Pentadbir Sistem ICT ANM; p. Sebarang kerosakan perkakasan ICT ANM hendaklah dilaporkan kepada Pentadbir Sistem ICT ANM untuk di baik pulih; q. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT ANM tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; s. Dilarang sama sekali mengubah kata laluan *administrator* yang telah ditetapkan oleh pihak ICT; t. Bertanggungjawab terhadap perkakasan, perisian dan	

	maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; u. Memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; dan v. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO ANM.	
DK050202	Media Storan	
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti 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 daripada 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	Pentadbir Sistem ICT, Pengguna

	daripada dipecahkan, api, air dan medan magnet; e. Media storan dan peralatan backup hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; f. Akses dan pergerakan kepada media storan perlu direkodkan; g. Perkakasan backup hendaklah diletakkan di tempat yang terkawal; dan h. Mengadakan salinan atau penduaan (*data backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	
DK050203	Media Perisian dan Aplikasi	
	Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a. Hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan di Jabatan; 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.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT

DK050204	Perkakasan Tanpa Penyeliaan (*Unattended Equipment*)	
	Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Pengguna
DK050205	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 pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset, Pentadbir Sistem ICT

DK050206	Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Perkakasan yang dibawa keluar premis ANM merangkumi :- a. Penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan b. Penempatan perkakasan secara kekal di sesebuah agensi lain. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a. Mendapatkan kelulusan Pegawai Aset/ Pentadbir Sistem ICT ANM bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan.	Pegawai Aset, Pengguna
DK050207	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 ANM; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh ANM bagi membawa masuk/ keluar peralatan; dan c. Memastikan peralatan yang dibawa keluar tidak mengandungi maklumat Kerajaan.	Pegawai Aset, Pengguna

DK050208	Pelupusan	
	Pelupusan melibatkan semua peralatan ICT ANM 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 daripada kawalan ANM. Langkah-langkah seperti berikut hendaklah diambil :- a. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; b. Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan; c. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; d. Media storan (*internal/external hard disk*) hendaklah dikeluarkan dan disimpan di tempat yang telah dikhaskan dengan ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; e. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); f. Pelupusan peralatan ICT ANM boleh dilakukan secara berpusat/ tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa; g. Maklumat lanjut berhubung pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan 5 Tahun	Pentadbir Sistem ICT, Pegawai Aset

	2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA); h. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut :- i. Menyimpan mana-mana peralatan ICT ANM 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 ANM; iii. Membawa keluar dari pejabat mana-mana peralatan ICT ANM yang hendak dilupuskan dalam tempoh proses pelupusan; dan iv. Melupuskan sendiri peralatan ICT tanpa melalui prosedur pelupusan yang ditetapkan. i. Semua Pengguna ICT ANM 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.	Pengguna
DK050209	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* bermaksud tidak meninggalkan sebarang maklumat penting di atas meja apabila pengguna tidak berada di tempatnya. *Clear Screen* bermaksud tidak memaparkan sebarang	Pengguna

	maklumat penting di paparan skrin apabila pengguna tidak berada di tempatnya. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut :- a. Menggunakan kemudahan kata laluan *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.	
DK0503 Keselamatan Persekitaran		
Objektif : Melindungi aset ICT ANM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
DK050301	Kawalan Persekitaran	
	Bagi mengelakkan kerosakan terhadap pejabat dan aset ICT ANM, 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	Pengurus ICT, ICTSO

	kecemasan; c. Penggunaan alat pencegahan kebakaran hendaklah mengikut keperluan dan piawaian yang ditetapkan serta bersesuaian dengan tempat, dokumen dan peralatan yang hendak dilindungi; 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 keselamatan dan kebakaran hendaklah diselenggara bagi memastikan ia dapat berfungsi dengan baik. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
DK050302	Kabel Rangkaian	
	Kabel rangkaian hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :- a. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; b. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; dan c. Melindungi laluan pemasangan kabel sepenuhnya bagi	Pentadbir Rangkaian

	mengelakkan ancaman kerosakan dan *wire tapping*.	
DK050303	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 ANM 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 di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	Pengurus ICT, ICTSO
DK050304	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 Pelan Tindakan Kecemasan ANM; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada pegawai yang berkenaan.	Pengguna
DK0504 Keselamatan Dokumen dan Sistem Dokumentasi		
DK050401	Dokumen	
	Bagi memastikan integriti maklumat, semua pengguna	Pentadbir

	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; dan f. Pelupusan dokumen hendaklah mengikut prosedur kerajaan yang telah ditetapkan di bawah Akta Arkib Negara 2003 (Akta 629), Akta Rahsia Rasmi dan Arahan Keselamatan.	Sistem ICT, 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.		
DK0601 Pengurusan Prosedur Operasi		
DK060101	Pengendalian Prosedur	
	Perkara yang perlu dipatuhi adalah seperti berikut :- a. Semua prosedur keselamatan ICT ANM yang diwujud, 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.	Pentadbir Sistem ICT
DK060102	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; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau	Pentadbir Sistem ICT

	pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
DK060103	Pengasingan Tugas dan Tanggungjawab	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggung jawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan dan rangkaian yang digunakan bagi tugas membangun, mengemaskini, dan menguji aplikasi hendaklah diasingkan daripada perkakasan dan rangkaian yang digunakan di dalam persekitaran *production*.	Pengurus ICT, ICTSO, Pentadbir Sistem

DK0602 Perancangan dan Penerimaan Sistem		
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
DK060201	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, Pentadbir Sistem ICT
DK060202	Penerimaan Sistem	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO, Pentadbir Sistem ICT
DK0603 Perisian Berbahaya		
Objektif : Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.		
DK060301	Perlindungan dari Perisian Berbahaya	
	Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus, Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen;	ICTSO, Pentadbir Sistem ICT

	c. Mengimbas semua perisian, sistem, media storan dan kepilan fail (*attachment*) dengan *antivirus* yang telah disediakan oleh jabatan sebelum menggunakannya; d. Mengemas kini *pattern antivirus* 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.	
DK0604 Housekeeping		
Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa boleh diakses.		
DK060401	Salinan Penduaan (*Backup*)	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan (*backup*) seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan.	Pentadbir Sistem ICT

	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 sistem penduaan sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan d. Backup hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan backup bergantung pada tahap kritikal maklumat.	
DK060402	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 ANM.	Pentadbir Sistem ICT
DK0605 Pengurusan Rangkaian		
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
DK060501	Kawalan Infrastruktur Rangkaian	
	Infrastruktur rangkaian mestilah dikawal dan diuruskan	Pentadbir

	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 pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk; 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 ANM; g. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat ANM; h. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; i. Sebarang penyambungan rangkaian yang bukan di bawah kawalan ANM tidak dibenarkan kecuali dengan kebenaran ICTSO; j. Semua pengguna hanya dibenarkan menggunakan	Rangkaian

	rangkaian ANM sahaja. Penggunaan modem dan rangkaian ANM secara serentak adalah dilarang sama sekali; k. Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan; dan l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
DK0606 Pengurusan Media		
Objektif : Melindungi aset ICT ANM daripada kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.		
DK060601	Penghantaran dan Pemindahan	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT terlebih dahulu.	Pengguna
DK060602	Prosedur Pengendalian Media	
	Perkara yang perlu dipatuhi adalah seperti berikut :- a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan 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; dan	Pentadbir Sistem ICT, Pengguna

	f. Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
DK060603	Pengurusan Penghantaran dan Penerimaan Maklumat	
	Pengurusan Penghantaran dan Penerimaan Maklumat bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin. Langkah-langkah bagi Pengurusan Penghantaran dan Penerimaan Maklumat adalah seperti berikut :- a. Polisi, prosedur dan kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk penghantaran dan penerimaan maklumat serta perisian di antara ANM dengan pihak luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan; 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 ANM.	Pentadbir Sistem ICT

DK0607 Keselamatan Komunikasi		
Objektif : Melindungi aset ICT ANM melalui sistem komunikasi yang selamat.		
DK060701	Mel Elektronik (E-mel)	
	Penggunaan e-mel ANM 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. Hanya warga ANM sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi ANM; b. Pentadbir E-mel perlu menetapkan had minimum kuota peti mel (*mailbox*); c. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh ANM sahaja boleh digunakan. d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; e. Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan; f. Setiap e-mel yang disediakan perlu mematuhi format yang telah ditetapkan oleh ANM; g. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; h. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima	Pentadbir E-mel, Pengguna

adalah betul;

i. Penggunaan fail kepilan (*attachment*) dibuat sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

j. Penghantaran lampiran dalam format/extension " *.exe, *.bat, *.hta, *.cmd dan *.com" tidak dibenarkan;

k. Mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

l. Mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

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

n. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

o. Tentukan tarikh dan masa sistem komputer adalah tepat;

p. Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*;

q. Seksyen Sumber Manusia perlu memaklumkan sebarang status pengguna (bertukar Jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke ANM bagi tujuan pengemaskinian e-mel yang terlibat;

r. Pengguna adalah mewakili diri sendiri dan

	bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik; dan s. Menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi *Universal Resource Location* (URL) atau kaedah pemanpatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan.	
DK060702	Perkhidmatan E-Dagang	
	Bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya. a. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pentadbir Sistem ICT
DK060703	Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
	Memastikan pelaksanaan dan penyenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	ICTSO, Pentadbir Sistem ICT, 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 menyelenggarakan dan menambahbaikkan polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
DK060704	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;	Pentadbir Sistem ICT

	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 ANM atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	
DK060705	Pengauditan ICT	
	Pentadbir Sistem ICT mestilah bertanggungjawab merekod dan menganalisis : a. Sebarang percubaan pencerobohan kepada sistem ICT ANM; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); 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;	ICTSO, Pentadbir Sistem ICT

	g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran alamat IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. 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 seseuatu laporan yang akan disediakan; b. Proses pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c. Sekiranya hasil laporan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan. Semua proses dan hasil laporan adalah SULIT.	

PERKARA 07 KAWALAN CAPAIAN

Objektif		
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT ANM.		
DK0701 Dasar Kawalan Capaian		
DK070101	Keperluan Dasar	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Sistem ICT
DK0702 Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas aset ICT ANM.		
DK070201	Akaun Pengguna	
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan langkah-langkah berikut hendaklah dipatuhi:- a. Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b. Akaun pengguna (*user id*) mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan yang ditetapkan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang (kecuali mendapat	Pengguna

	kebenaran); dan e. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut :- i. Pengguna bercuti panjang; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
DK070202	Hak Capaian (*Privilege*)	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
DK070203	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; c. Panjang kata laluan mestilah sekurang-kurangnya 10 aksara dengan gabungan antara huruf, nombor dan aksara khas manakala kata laluan bagi pembangunan aplikasi sistem yang baru mestilah sekurang-kurangnya dua belas (12) aksara dengan kombinasi aksara, angka dan aksara khas;	Pentadbir Sistem ICT, Pengguna

	d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* 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 (kecuali pada sistem/ aplikasi tertentu); dan h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna.	
DK070204	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 pengeluar kad.	Pengguna ANM yang terlibat

DK0703 Kawalan Capaian		
Objektif : Menghalang capaian yang tidak sah dan tanpa kebenaran serta boleh menyebabkan kerosakan.		
DK070301	Kawalan Capaian Rangkaian	
	Perkara yang perlu dipatuhi adalah seperti berikut :- a. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian dalaman (Intranet) dan rangkaian Awam (DMZ). b. Memastikan pengguna membuat capaian pada sistem yang dibenarkan sahaja; c. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; dan d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT
DK070302	Capaian Jarak Jauh	
	Capaian jarak jauh yang dimaksudkan merangkumi: i. Capaian daripada sistem rangkaian dalaman; dan ii. Capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *troubleshooting*. a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah *Remote Access* mestilah menggunakan kaedah penyulitan (*encryption*); b. Lokasi bagi akses ke sistem ICT ANM hendaklah dipastikan selamat ; dan c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada ICTSO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas	Pentadbir Sistem ICT, Pengguna

	penggunaan kemudahan ini.	
DK070303	Capaian Internet	
	a. Penggunaan Internet di ANM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian ANM;	Pentadbir Rangkaian
	b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;	ICTSO
	c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pentadbir Rangkaian
	d. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video streaming, chat, downloading*, dan lain-lain aktiviti yang dikenalpasti) adalah perlu bagi menguruskan penggunaan bandwidth yang maksimum dan lebih berkesan;	
	e. Penggunaan proksi yang telah ditetapkan oleh ANM bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan;	
	f. Penggunaan modem peribadi untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali di pejabat;	Pengguna
	g. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :- i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video/audio,	

	lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. h. Pengguna hendaklah berhenti dan memutuskan talian dengan serta merta sekiranya menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan.	
DK0704 Kawalan Capaian Sistem dan Aplikasi		
Objektif : Melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
DK070401	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 kepada 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	Pentadbir Sistem ICT

	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 :- 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 yang kukuh; d. Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan e. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
DK070402	Sistem Maklumat dan Aplikasi	
	Capaian sistem dan aplikasi di ANM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi :-	Pentadbir Sistem ICT

	a. Pengguna hanya 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. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Memastikan kawalan sistem adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
DK0705 Audit		
DK070501	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 identiti 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;	Pentadbir Sistem ICT

	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; dan f. Aktiviti perlindungan daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian 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.		
DK0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
DK080101	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 memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	ICTSO, Pentadbir Sistem ICT
DK080102	Pengesahan Data Input	
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem ICT

DK080103	Kawalan Prosesan	
	Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem ICT
DK080104	Pengesahan Data Output	
	Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem ICT
DK0802 Kriptografi		
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
DK080201	Pengurusan Infrastruktur Kunci Awam (PKI)	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengguna
DK0803 Fail Sistem		
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
DK080301	Kawalan Fail Sistem	
	Perkara yang perlu dipatuhi adalah seperti berikut :- a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;	Pentadbir Sistem ICT

	d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e. Data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.	
DK0804 Pembangunan dan Sokongan Sistem		
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
DK080401	Kawalan Perubahan	
	Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem ICT
DK080402	Pembangunan Secara *Outsource*	
	Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh ICTSO. *Source code* adalah menjadi hak milik ANM.	Pentadbir Sistem ICT
DK080403	Kawalan dari Ancaman Teknikal	
	Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan; b. Menilai tahap pendedahan bagi mengenalpasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	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 ANM dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej ANM dan sistem penyampaian perkhidmatan.

DK0901 Pengurusan Insiden Keselamatan ICT		
DK090101	Mekanisme Pelaporan Insiden Keselamatan ICT	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera :- a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberikuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut :- i. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO untuk pengendalian dan	Pengguna ICTSO, Pengguna

	pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. ICTSO akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya. ii. 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 sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh. iii. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan 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.	Pengguna CIO, ICTSO
DK090102	Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT	
	Pentadbir Sistem ICT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan GCERT. a. Pentadbir Sistem ICT menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari PRISMA atau laporan daripada sumber luar. Seterusnya,	ICTSO, Pentadbir Sistem ICT

	maklumat tentang insiden akan didaftarkan. b. 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. c. Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan perlu dihantar bagi mendapatkan maklum balas GCERT MAMPU. d. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan perlu dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. Pentadbir Sistem ICT seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Pemulihan Bencana ICT/ *Disaster Recovery Plan* (DRP) ICT perlu diaktifkan atau sebaliknya. Pengesahan perlu dihantar kepada CIO bagi mengaktifkan DRP. e. Laporan insiden yang tidak memerlukan DRP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.	
DK090103	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	ICTSO, Pentadbir Sistem ICT

	berlaku atau yang memberi kesan serta impak yang tinggi kepada ANM; 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 dipertanggungjawabkan; 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 daripada 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.		
DK1001 Dasar Kesinambungan Perkhidmatan		
DK100101	Pelan Kesinambungan Perkhidmatan/ *Business Continuity Pelan* (BCP)	
	Pelan Kesinambungan Perkhidmatan/ *Business Continuity Plan* (BCP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian :- a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. Membuat penduaan; dan f. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	ICTSO, Pengurus ICT

BCP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut :

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b. Senarai Pegawai ANM dan vendor berserta nombor yang boleh dihubungi (faksimili, telefon, e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai yang tidak dapat hadir untuk menangani insiden;

c. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahu mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

ANM hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.

DK100102	Pengurusan Kesinambungan Perkhidmatan/ *Business Continuity Management* (BCM)	
	Pengurusan Kesinambungan Perkhidmatan/ *Business Continuity Management* (BCM) adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej ANM terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan ANM di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT ANM.	KP, Pengurus ICT, ICTSO

PERKARA 11 PEMATUHAN

Objektif		
Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada DKICT ANM.		
DK1101 Pematuhan dan Keperluan Perundangan		
DK110101	Pematuhan Dasar	
	DKICT ANM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa hendaklah dibaca, difahami dan dipatuhi. Semua aset ICT ANM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan.	Pengguna
DK110102	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
DK110103	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	ICTSO

	mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
DK110104	Keperluan Perundangan dan Peraturan	
	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	Pengguna

	Awam"; 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 Arkib Negara 2003 (Akta 629); n. Akta Rahsia Rasmi 1972; o. Akta Tandatangan Digital 1997; p. Akta Jenayah Komputer 1997; q. Akta Hak cipta (Pindaan) Tahun 1997; r. Akta Komunikasi dan Multimedia 1998; s. Arahan Teknologi Maklumat 2007; t. Perintah-Perintah Am; dan	

	u. Arahan Perbendaharaan.	
DK1102 Tindakan Tatatertib		
Objektif : Meningkatkan kesedaran dan pematuhan ke atas DKICT ANM.		
DK110201	Pelanggaran Dasar / Perundangan	
	Pelanggaran DKICT ANM dan semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan Perintah-perintah Am Bab "D" – Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) akan dikenakan tindakan tatatertib.	Pengguna

GLOSARI	
ANM	Arkib Negara Malaysia merangkumi Ibu Pejabat, Cawangan Negeri, Memorial/ Galeria/ Pustaka/ Rumah Kelahiran.
Aksara khas	Contoh : ! @ # $ % ^ & * ? } >
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 Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
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.
BCM	*Business Continuity Management.* Pengurusan Kesinambungan Perkhidmatan.
BCP	*Business Continuity Plan.* Pelan Kesinambungan Perkhidmatan.
CIO	*Chief Information Officer.* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Denial of service	Halangan pemberian perkhidmatan.
DKICT ANM	Dasar Keselamatan ICT ANM.
Downloading	Aktiviti muat-turun sesuatu perisian/ aplikasi/ fail/ dokumen.
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	I*CT Security Officer.* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunkasi atau ancaman kemungkinan berlaku kejadian tersebut.
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.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan. Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan. Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya : *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan

	serangan.
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman daripada pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (*standard format*) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
LAN	*Local Area Network.* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Modem	*MOdulator DEModulator.* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau Jabatan.
Pihak Ketiga	Kontraktor, Pembekal, Pakar Runding dan pihak-pihak lain yang berkepentingan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Pusat Data	Pusat Data ANM merangkumi dua (2) pusat data utama iaitu di Bangunan Menara Ilmu dan Bangunan Pusat Pendokumentasian dan Pemeliharaan Bahan Audio Visual (PPPAV).
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenran akan membhayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada

	Malaysia.
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negeraa tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/ Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threats	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conferencing	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT
ARKIB NEGARA MALAYSIA

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

☐ Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT; dan

Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tanda Tangan Pegawai)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
b.p Ketua Pengarah
Arkib Negara Malaysia

Tarikh : .....

Lampiran B

PERAKUAN UNTUK DITANDATANGANI OLEH KONTRAKTOR YANG TERLIBAT DENGAN PROJEK KERAJAAN MENURUT AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu.Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila tamat projek Kerajaan.

Tandatangan : ----------

Nama dengan Huruf Besar : _____

Jawatan : _____

Syarikat : _____

No. Kad Pengenalan : _____

Tarikh : _____

Disaksikan Oleh : ----------

(Arkib Negara Malaysia) (Tandatangan)

Nama dengan Huruf Besar : _____

Jawatan : _____

Jabatan : ARKIB NEGARA MALAYSIA

No. Kad Pengenalan : _____

Tarikh : _____

Cop Jabatan :

Lampiran B

DECLARATION TO BE SIGNED BY CONTRACTORS ENGAGED ON GOVERNMENT PROJECTS IN RESPECTS OF THE OFFICIAL SECRETS ACT 1972

I hereby acknowledge that my attention has been drawn to the provisions of the Official Secrets Act 1972 (Act 88), as amended, and that fully understand the implications contained thereof. In particular I understand that to communicate to unauthorised person, to use or having in possession without authorisation any classified materials, and failure to take reasonable care of classified materials, I shall be guilty of an offence under this Act and punishable with imprisonment for life.

I understand that all official information acquired by me in the service of His Majesty the Yang di-Pertuan Agong or any Government in the Federation, is the property of the Government and is not to be divulged, published, or communicated, whether orally or in writing, to any other person in any form, except in the course of my official duties, whether during or after my service with His Majesty the Yang di-Pertuan Agong or Government in the Federation without the previous sanction in writing of the relevant authority. I undertake to sign a further declaration to this effect on completion of the Government Project.

Signature : _____
Name In Capital Letter : _____
Identification Card No : _____
Position : _____
Company : _____
Date : _____

Witnessed By : _____
(National Archives of Malaysia) (Signature)
Name In Capital Letter : _____
Position : _____
Agency : NATIONAL ARCHIVES OF MALAYSIA
Identification Card No : _____
Date : _____
Agency Stamp :