DASAR KESELAMATAN ICT

NEGERI KEDAH DARUL AMAN

27 DISEMBER 2012

VERSI 3.0

ISI KANDUNGAN

GLOSARI **I – iv**

PENDAHULUAN **1 – 2**
- Wawasan
- Misi
- Objektif
- Skop

PERNYATAAN DASAR **3 – 4**

PRINSIP DASAR KESELAMATAN ICT **5 – 8**

PENILAIAN RISIKO KESELAMATAN ICT **9**

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR **10**
- Pelaksanaan Dasar
- Penyebaran Dasar
- Penyelenggaraan Dasar
- Pengecualian Dasar

PERKARA 02 ORGANISASI PENGURUSAN KESELAMATAN ICT **11 – 17**
- Objektif
- Setiausaha Kerajaan Negeri
- Ketua Pegawai Maklumat (CIO)
- Pegawai Keselamatan ICT (ICTSO)
- Pengurus ICT
- Pentadbir Sistem ICT
- Pengguna
- Keperluan Keselamatan Kontrak Dengan Pihak Ketiga
- Jawatankuasa Pemandu Keselamatan ICT
- Jawatankuasa CERT Negeri
- Jawatankuasa CERT Agensi

PERKARA 03 (a) PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN **18 – 19**
- Objektif
- Mekanisme Pelaporan
- Pengurusan Maklumat Insiden Keselamatan ICT
    - Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

PERKARA 03 (b) PENGURUSAN RISIKO KESELAMATAN ICT **20**
- Objektif
- Pengurusan Risiko Keselamatan ICT

Security Posture Assessment (SPA)

PERKARA 04 KLASIFIKASI DAN PENGENDALIAN MAKLUMAT **21 – 22**
Objektif
Klasifikasi Maklumat
Pengendalian Maklumat
Inventori Aset

PERKARA 05 KESELAMATAN SUMBER MANUSIA **23 – 25**
Objektif
Terma dan Syarat Perkhidmatan
Menangani Insiden Keselamatan ICT
Latihan Kesedaran Keselamatan ICT
Kejuruteraan Sosial
Perlanggaran Dasar

PERKARA 06 KESELAMATAN FIZIKAL DAN PERSEKITARAN **26 – 32**
Objektif
Perimeter Kawalan Fizikal
Kawalan Fizikal
Kawalan Akses Pusat Data / Bilik Server
Kawalan Persekitaran
Kawalan Perkhidmatan Dan Penyelenggaraan
Kawalan Peralatan
Kawalan Dokumen

PERKARA 07 KESELAMATAN OPERASI, KOMUNIKASI DAN RANGKAIAN **33 – 46**
Objektif
Perancangan Dan Penerimaan Sistem
Kawalan Perisian
Housekeeping
Perlindungan dari Perisian Berbahaya
Pengurusan Infrastruktur Rangkaian
Pengurusan Media
Keselamatan Komunikasi
    Perkhidmatan Mel Elektronik (e-Mel)
    Perkhidmatan Melayari Internet
    Perkhidmatan Laman Web
Pemantauan
    Pengauditan dan Forensik ICT
    Jejak Audit
    Sistem Log
    Pemantauan Log
Lain-Lain Perkhidmatan

PERKARA 08 KAWALAN CAPAIAN **47 – 54**
Objektif
Akaun Pengguna
Kawalan Akses
Perakaunan Dan Jejak Audit (Audit Trail)
Kawalan Capaian Sistem Maklumat Dan Aplikasi
Clear Desk dan *Clear Screen*
Kawalan Capaian Rangkaian
Capaian Rangkaian
Capaian Internet
Kawalan Capaian Sistem Pengoperasian
Capaian Sistem Pengoperasian
Kad Pintar
Keselamatan Komputer Mudah Alih / Riba
Aset ICT

PERKARA 09 KESELAMATAN SISTEM APLIKASI **55 – 57**
Objektif
Keselamatan Dalam Membangunkan Sistem Dan Aplikasi
Pengesahan Data Input Dan Output
Kriptografi (Cryptography)
Kawalan Fail Sistem
Pembangunan Dan Proses Sokongan
Kawalan Teknikal Keterdedahan (*Vulnerability*)
Kawalan dari Ancaman Teknikal

PERKARA 10 PELAN KESINAMBUNGAN PERKHIDMATAN DAN PEMULIHAN BENCANA **58**
Objektif
Pelaksanaan

PERKARA 11 PEMATUHAN **59 – 60**
Objektif
Pematuhan Dasar
Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal
Pematuhan Keperluan Audit
Keperluan Perundangan Dan Peraturan

RUJUKAN **62**

GLOSARI

TERMINOLOGI	MAKSUD
Arahan Keselamatan	Panduan mengenai peraturan-peraturan keselamatan yang perlu dipatuhi oleh semua Kakitangan kerajaan.
Aset ICT	Komponen-komponen yang terdiri daripada Perkakasan, perisian, aplikasi dan sistem rangkaian ICT.
Audit Trail	Satu proses untuk mengenalpasti semua aktiviti yang dilakukan oleh komputer dalam memproses kemasukan data, penjanaan output dan segala aktiviti yang terlibat di antaranya.
Autentikasi	Satu kaedah untuk mengenalpasti identiti pengguna, peralatan atau entiti dalam sistem komputer sebelum kebenaran diberikan untuk mengakses kepada sesuatu sistem.
Biometric	Kaedah yang digunakan untuk pengecaman identiti individu melalui pengesanan seperti cap jari, suara dan retina.
Business Continuity Planning (BCP)	Pelan tindakan untuk merancang aktiviti-aktiviti kesinambungan perniagaan atau perkhidmatan.
Central Processing Unit (CPU)	Unit Pemprosesan Utama iaitu yang mengandungi pemproses, cakera keras, ingatan dan papan utama.
Computer Emergency Response Team (CERT)	Pasukan yang akan bertindak sekiranya berlaku bencana atau perkara-perkara yang tidak diingini.
Hub	Peralatan rangkaian menghubung satu stesen kerja dengan stesen kerja yang lain.
Intrusion Detection System (IDS)	Satu peralatan yang digunakan untuk memantau atau merekod cubaan pencerobohan.
Internet	Perkhidmatan informasi secara global yang menghubungkan semua pengguna seluruh dunia melalui satu protocol rangkaian.
Information Security	Proses dan mekanisme untuk melindungi maklumat.
Jawatankuasa Pemandu ICT Negeri	Jawatankuasa ICT Tertinggi di peringkat Kerajaan Negeri Kedah yang diketuai oleh Setiausaha

	Kerajaan Negeri dan dianggotai oleh semua Ketua-Ketua Jabatan di setiap Jabatan / Agensi Negeri.
Kata Laluan	Satu kumpulan karektor atau gabungan karektor dan nombor yang mengesahkan pengenalan diri dan digunakan sebagai satu syarat untuk capaian kepada sesuatu sistem.
Kawalan Akses	Pengawasan terhadap pencapaian untuk perkakasan, perisian dan rangkaian.
Keselamatan Fizikal	Faktor-faktor keselamatan luaran yang perlu diambilkira untuk menjamin keselamatan perkakasan dan perisian.
Keselamatan Sumber Manusia	Persekitaran yang disediakan bagi menjamin keselamatan kakitangan.
Ketua Pegawai Maklumat (CIO)	Pegawai yang dilantik dan bertanggungjawab dalam perancangan dan pembangunan ICT sesebuah agensi kerajaan.
Kriptografi	Kaedah untuk menukar maklumat biasa kepada format yang tidak boleh difahami.
Lightning Arrestor	Peralatan yang digunakan bagi melindungi perkakasan elektrik dari terkena kilat.
Mail Server	Pelayan yang digunakan sebagai platform oleh sesebuah organisasi untuk menguruskan penerimaan dan penghantaran e-mel.
Maklumat Terperingkat	Maklumat rasmi yang telah diklasifikasikan mengikut klasifikasi rahsia besar, rahsia, sulit dan terhad. Maklumat ini boleh didapati dalam bentuk percetakan atau di dalam bentuk digital.
Media Storan	Peralatan untuk menyimpan maklumat digital.
Modem	Satu peranti yang membenarkan komputer menghantar maklumat melalui rangkaian telekomunikasi.
Mel Elektronik	Mel yang dihantar secara elektronik.
Pegawai Keselamatan ICT (ICTSO)	Pegawai yang bertanggungjawab untuk menjaga keseluruhan keselamatan maklumat.

Pentadbir Sistem ICT	Pegawai yang bertanggungjawab sebagai Pengurus Projek / Pentadbir Rangkaian / Pentadbir Sistem Aplikasi / Pentadbir Pangkalan Data / Pengurus Pusat Data.
Penyenggaraan Pembetulan (Corrective Maintenance)	Pembaikan yang dibuat terhadap perkakasan dan perisian apabila berlaku kerosakan.
Penyulitan	Proses yang berlaku ketika penukaran maklumat dari asal kepada yang tidak boleh difahami.
Perisian	Merujuk kepada semua aset-aset digital ICT.
Perkakasan	Merujuk kepada semua aset-aset fizikal ICT.
Phishing	Merujuk kepada kaedah memanipulasi kelemahan manusia untuk mendapatkan maklumat dengan menggunakan pemujukan, pengaruh dan penipuan.
Pihak Luar / Ketiga	Kontraktor, pembekal dan lain-lain pihak yang berkepentingan.
Power Surge	Aliran kuasa elektrik yang melebihi had.
Preventive Maintenance	Penyelenggaraan pencegahan berjadual untuk melindungi perkakasan, perisian atau operasi.
Pusat Teknologi Maklumat dan Komunikasi Negeri (PTMK)	Pusat Teknologi Maklumat dan Komunikasi Negeri (PTMK) adalah satu bahagian di bawah Pejabat Setiausaha Kerajaan Negeri Kedah yang bertanggungjawab dalam perancangan dan pembangunan ICT.
Rangkaian Dalaman (Private Network)	Rangkaian komputer persendirian yang digunakan bagi tujuan komunikasi dan hubungan dalam organisasi.
Rangkaian Awam (Public Network)	Rangkaian komputer awam yang digunakan secara bersama oleh semua Jabatan / Agensi Negeri untuk membuat capaian ke Internet.
Router	Sejenis peralatan rangkaian yang digunakan untuk menghubungkan antara satu rangkaian dengan rangkaian lain.
Risk Assessment	Analisa risiko untuk mengenalpasti kelemahan-kelemahan yang terdapat dalam sistem yang boleh memberi ancaman kepada keselamatan.

Secured Network	Sistem rangkaian terselamat di mana maklumat yang melaluinya dikawal dan dilindungi.
UPS	Peranti yang mengandungi bateri yang menyimpan kuasa yang bertujuan untuk mengambil alih peranan kuasa elektrik sekiranya berlaku gangguan bekalan kuasa dalam tempoh terhad.
Virtual Private Network (VPN)	Rangkaian Maya Persendirian yang menggunakan infrastruktur telekomunikasi awam, tetapi masih mengekalkan pemilikan (privacy) melalui protokol tertentu dan lain-lain prosedur keselamatan.
Web Server	Pelayan yang digunakan sebagai platform aplikasi web oleh sesebuah organisasi untuk penyampaian maklumat dan perkhidmatan kepada pelanggan melalui internet.

PENDAHULUAN

Penggunaan ICT di kalangan masyarakat dunia semakin menyerlah dengan pelbagai inovasi peralatan komunikasi ICT. Segala maklumat yang diperlukan hanya diperoleh semudah di hujung jari. Kesan penggunaan ICT ini telah mengubah budaya kerja organisasi. Sementara berbangga dengan kemajuan yang dicapai, semua warga Kerajaan Negeri Kedah Darul Aman juga perlu peka terhadap isu keselamatan ICT terutama dari segi peranan, tanggungjawab dan kawalan penggunaannya. Penekanan ke atas kesedaran dan tahap keselamatan ICT adalah penting dan perlu diberi perhatian yang serius disebabkan oleh dua faktor.

Faktor pertama ialah keselamatan ICT merupakan tanggungjawab bersama untuk memastikan sistem ICT yang dikendalikan adalah selamat daripada sebarang penyalahgunaan dan ancaman pencerobohan.

Faktor kedua ialah kewujudan penggunaan pelbagai teknologi dan platform sistem pengoperasian. Keadaan ini menjadikan ia lebih terbuka kepada ancaman keselamatan. Adalah penting di sini supaya penyimpanan maklumat dan penyebaran maklumat perlu dibatasi supaya ia dapat dikawal dengan lebih berkesan.

Dasar Keselamatan ICT Negeri Kedah mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Negeri kedah.

WAWASAN

Mewujudkan persekitaran sistem ICT yang komprehensif, selamat, berkesan, stabil dan boleh dipercayai (reliable).

MISI

Untuk mencapai tahap keselamatan ICT yang menyeluruh bagi menyokong peranan Kerajaan Negeri dalam melindungi kepentingan strategik negeri dan aset-asetnya.

OBJEKTIF

a) Menghebahkan pendirian pihak pengurusan untuk mendukung pelaksanaan keselamatan ICT.
b) Menyediakan Dasar Keselamatan ICT yang komprehensif, sesuai dengan perubahan semasa dan mampu digunapakai oleh semua peringkat pengurusan dan pengguna.
c) Menjamin kesinambungan operasi Kerajaan Negeri dan meminimumkan kerosakan atau kemusnahan.
d) Melindungi kepentingan aset-aset yang bergantung kepada sistem ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi serta mencegah aktiviti penyalahgunaan.

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh : fail, dokumen, data elektronik, maklumat perbualan), perisian (contoh : aplikasi dan sistem perisian) dan fizikal (contoh : komputer / peralatan komunikasi dan media magnet). Dasar ini adalah terpakai oleh semua pengguna di Jabatan / Agensi Negeri termasuk kakitangan, pembekal, dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Jabatan / Agensi Negeri.

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:

i. Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah
ii. Menjamin setiap maklumat adalah tepat dan sempurna
iii. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna
iv. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah

Dasar Keselamatan ICT Negeri Kedah 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:

i. Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran
ii. Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan
iii. Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal
iv. Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya
v. 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.

PRINSIP DASAR KESELAMATAN ICT

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

a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu mengikut dasar perlu mengetahui sahaja. Pertimbangan akses di bawah prinsip ini hendaklah berteraskan kepada klasifikasi maklumat dan tapisan keselamatan yang dihadkan kepada pengguna.

Klasifikasi maklumat hendaklah mematuhi ”Arahan Keselamatan Kerajaan”. Maklumat ini dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Penggunaan encryption, tandatangan digital atau sebarang mekanisma lain yang boleh melindungi maklumat mestilah juga dipertimbangkan. Dasar klasifikasi ke atas sistem aplikasi juga hendaklah mengikut klasifikasi maklumat yang sama.

b) Hak Akses Minimum

Hak akses kepada pengguna hanya diberikan pada tahap yang paling minimum iaitu untuk membaca, melihat atau mendengar sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah dan membatalkan sesuatu data atau maklumat elektronik.

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mempunyai keupayaan mengesan dan mengesahkan pengguna boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna merangkumi perkara berikut :

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 piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penyelenggaraan, penghantaran, penyampaian, pertukaran dan pemusnahan.

d) Pengauditan Keselamatan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Pentadbir Sistem perlu memastikan semua log / audit trail yang dijanakan oleh aset ICT berkaitan keselamatan disimpan sekurang-kurangnya 6 bulan. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian apabila diperlukan. Ketua Jabatan atau setaraf boleh mempertimbangkan penggunaan perisian tambahan bagi menentukan ketepatan dan kesahihan log / audit trail.

e) Pemulihan

Pemulihan sistem ICT amat diperlukan untuk memastikan kebolehsediaan, kebolehcapaian dan kerahsiaan. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan hendaklah dilakukan melalui tindakan berikut :

i. Pelan Pemulihan Bencana Sistem ICT hendaklah diuji sekurang-kurangnya sekali setahun. Ketua Jabatan atau setaraf dikehendaki menentukan perkara ini dilaksanakan.
ii. Pentadbir sistem dikehendaki melaksanakan proses backup secara berkala, ujian pemulihan (restore) bagi sistem ICT yang terlibat.

f) Pematuhan

Pematuhan Dasar Keselamatan ICT adalah berdasarkan tindakan berikut :

i. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.

ii. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
iii. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. PTMK / Unit ICT Agensi Negeri berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan Negeri / Agensi berkaitan.
iv. Menguatkuasakan amalan melapor sebarang insiden yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan / pemulihan.

g) Pengasingan

Pengasingan fungsi/tugas perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi/tugas juga perlu dilakukan di antara pentadbir sistem, pentadbir rangkaian dan bahagian pentadbiran pejabat.

h) Integriti

Data dan maklumat hendaklah tepat, lengkap dan sentiasa terkini. Sebarang perubahan terhadap data hendaklah dilaksanakan oleh staf yang diberi kebenaran sahaja.

i) Autentikasi Dan Penyahsangkalan

Proses ini merupakan keupayaan bagi membuktikan bahawa sesuatu mesej atau maklumat tertentu telah dihantar oleh pemilik asal yang dikenalpasti. Setiap sistem ICT berangkaian hendaklah dilengkapi dengan sistem autentikasi yang secukupnya. Bagi sistem yang mengendalikan maklumat terperingkat, ciri penyahsangkalan hendaklah digunakan.

j) Perimeter Keselamatan Fizikal

Perimeter merujuk kepada keadaan persekitaran fizikal di mana aset-aset ICT dilindungi. Perimeter tersebut hendaklah dijaga dengan rapi bagi mengelakkan sebarang pencerobohan. Ketua Jabatan atau setaraf hendaklah memastikan proses ini dilaksanakan.

k) Pertahanan Berlapis (Defence in depth)

Pertahanan berlapis hendaklah diwujudkan untuk melindungi keselamatan aset ICT dari pencerobohan. Ketua Jabatan atau setaraf hendaklah menentukan sistem ICT mempunyai pertahanan berlapis yang lengkap mengikut teknologi semasa.

l) Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip tersebut. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan yang lain. Tindakan mempersepadukan prinsip yang telah dinyatakan perlu dilaksanakan bagi menjamin tahap keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

Pusat Teknologi Maklumat Negeri Kedah (PTMK) hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu PTMK perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dicapai bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

PTMK / Unit ICT jabatan hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat ICT termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utilitii dan sistem-sistem sokongan lain.

PTMK / Unit ICT jabatan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

PTMK perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian
2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi
3. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko
4. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Perkara 01 Pembangunan Dan Penyelenggaraan Dasar

1.0	Pelaksanaan Dasar	Tanggungjawab
	Pelaksanaan Dasar ini dijalankan oleh Setiausaha Kerajaan Negeri dibantu oleh Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan.	Setiausaha Kerajaan Negeri
2.0	Penyebaran Dasar	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan / Agensi Negeri (termasuk kakitangan, pembekal, pakar runding dll)	ICTSO
3.0	Penyelenggaraan Dasar	
	Dasar Keselamatan ICT Negeri ini 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 Dasar Keselamatan ICT : i. Kenalpasti dan tentukan perubahan yang diperlukan ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO masing-masing untuk dibentangkan kepada Jawatankuasa CERT Negeri bagi mendapatkan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Negeri iii. Perubahan yang telah dipersetujui oleh Jawatankuasa Pemandu ICT Negeri/CIO dimaklumkan kepada semua pengguna iv. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa	ICTSO
4.0	Pengecualian Dasar	
	Dasar Keselamatan ICT Negeri adalah terpakai kepada semua pengguna ICT Jabatan / Agensi dan tiada	Semua

	pengecualian diberikan	

Perkara 02 Organisasi Pengurusan Keselamatan ICT

1.0	Objektif	Tanggungjawab
	Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi	
2.0	Setiausaha Kerajaan Negeri	
	Peranan dan tanggungjawab adalah seperti berikut : i. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Negeri ii. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Negeri iii. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi iv. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Negeri	Setiausaha Kerajaan Negeri
3.0	Ketua Pegawai Maklumat (CIO)	
	Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO) di semua Jabatan dan Agensi Negeri adalah seperti berikut : i. Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT ii. Menentukan keperluan keselamatan ICT iii. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT iv. Memastikan setiap pegawai dan kakitangan	Ketua Pegawai Maklumat (CIO)

	menandatangani surat akuan mematuhi Dasar Keselamatan ICT Negeri v. Mengambil tindakan ke atas anggota yang melanggar Dasar Keselamatan ICT Negeri vi. Menguruskan tindakan ke atas insiden keselamatan yang berlaku sehingga keadaan pulih vii. Mengaktifkan Business Resumption Plan (BRP) jika perlu viii. Menentukan sama ada insiden keselamatan yang berlaku perlu dilaporkan kepada agensi penguatkuasa undang-undang / keselamatan	
4.0	Pegawai Keselamatan ICT (ICTSO)	
	Peranan dan tanggungjawab ICTSO di semua Jabatan / Agensi Negeri yang dilantik adalah seperti berikut : i. Mengurus program-program keselamatan ICT ii. Menguatkuasakan Dasar Keselamatan ICT iii. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua pengguna iv. Melaksanakan garis panduan, prosedur dan tatacara yang berkaitan selaras dengan keperluan Dasar Keselamatan ICT Negeri v. Menjalankan pengurusan risiko vi. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya vii. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian	Pegawai Keselamatan ICT (ICTSO)

	viii. Menentukan tahap keutamaan insiden, melaporkan insiden keselamatan ICT kepada Pasukan CERT Negeri dan memaklumkan kepada CIO serta mengambil langkah pemulihan awal ix. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan langkah-langkah baik pulih dengan segera x. Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Negeri xi. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT	
5.0	Pengurus ICT	
	Pengurus ICT bagi Negeri Kedah ialah Pengarah Pusat Teknologi Maklumat Negeri Kedah. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: i. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Kerajaan Negeri Kedah; ii. Menentukan kawalan akses pengguna terhadap aset ICT Negeri Kedah; iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Negeri.	
6.0	Pentadbir Sistem ICT	
	Peranan dan tanggungjawab Pentadbir Sistem ICT	

	adalah seperti berikut : i. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas ii. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT iii. Memantau aktiviti capaian harian pengguna iv. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta v. Menyimpan dan menganalisis rekod audit trail vi. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala	Pentadbir Sistem ICT
7.0	Pengguna	
	Peranan dan tanggungjawab pengguna adalah seperti berikut : i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT ii. Mengetahui dan memahami implikasi keselamatan ICT, kesan dan tindakannya iii. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat iv. Melaksanakan langkah-langkah perlindungan seperti berikut : a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan	Semua

	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 g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera vi. Menghadiri program-program kesedaran mengenai keselamatan ICT vii. Menandatangani surat akuan mematuhi Dasar Keselamatan ICT	
8.0	Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	
	Pihak ketiga perlu menandatangani dokumen-dokumen berikut bagi melindungi aset ICT kerajaan : i. Surat Akuan mematuhi Dasar Keselamatan ICT / Nondisclosure Agreement (NDA) Kandungan kontrak dengan pihak ketiga perlu merangkumi pematuhan terhadap : i. Dasar Keselamatan ICT	Semua

	ii. Perakuan Akta Rahsia Rasmi 1972 iii. Hak Harta Intelek Penggunaan outsourcing perlu dikawal daripada segi pelaksanaannya bagi menjamin keselamatan terhadap sistem yang akan dilaksanakan secara outsource. Kaedah pelaksanaan outsourcing adalah berdasarkan kepada Garis Panduan IT Outsource Agensi-Agensi Sektor Awam	
9.0	Jawatankuasa Pemandu Keselamatan ICT	
	Keahlian dan bidang rujukan jawatankuasa ini dilaksanakan di bawah Jawatankuasa Pemandu ICT. Tanggungjawab khusus berkaitan dengan aspek keselamatan ICT adalah seperti berikut : i. Merangka dasar, hala tuju, garis panduan dan piawaian keselamatan ICT ii. Meneliti, meluluskan dan menguatkuasakan Dasar Keselamatan ICT iii. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT iv. Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan v. Meluluskan inisiatif untuk peningkatan keselamatan ICT vi. Memantau ancaman-ancaman utama terhadap aset-aset ICT vii. Memastikan pengauditan sistem ICT dilaksanakan sekurang-kurangnya sekali setahun	Jawatankuasa Pemandu ICT
10.0	Jawatankuasa CERT Negeri	
	Skop tanggungjawab CERT Negeri merangkumi semua jabatan negeri di negeri Kedah Darul Aman. Keahlian	

	jawatankuasa ini adalah seperti berikut : Tugas dan tanggungjawab jawatankuasa ini adalah seperti berikut : i. Mengurus insiden keselamatan ICT peringkat negeri ii. Memberi nasihat teknikal kepada Jawatankuasa Pemandu ICT Negeri iii. Mengkaji semula Dasar Keselamatan ICT dari semasa ke semasa untuk dibentangkan kepada Jawatankuasa Pemandu ICT atau CIO iv. Melaksanakan ujian penembusan (pentest) bagi sistem ICT secara berkala bagi mengetahui kelemahan konfigurasi/skrip	Jawatankuasa CERT Negeri
11.0	Jawatankuasa CERT Agensi	
	Keahlian ditentukan oleh agensi masing-masing berpandukan kepada Pekeliling Am Bil. 4 Tahun 2006 dan pekeliling-pekeliling yang berkaitan	CIO Agensi dan Jawatankuasa CERT Agensi

Perkara 03 (a) Pengurusan Pengendalian Insiden Keselamatan

1.0	Objektif	Tanggungjawab
	Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
2.0	Mekanisme Pelaporan	
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah	Semua

	dilaporkan kepada ICTSO dan/atau CERT Negeri dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Timbul keraguan yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	
3.0	Pengurusan Maklumat Insiden Keselamatan ICT	
3.1	Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan 18ntegr. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Kerajaan Negeri. Bahan-bahan bukti berkaitan insiden keselamatan ICT	ICTSO

	hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

Perkara 03 (b) Pengurusan Risiko Keselamatan ICT

1.0	Objektif	Tanggungjawab
	Mengenalpasti tahap keselamatan, *vulnerabilities* dan kelemahan infrastruktur dan aset ICT untuk proses pembaikan dan peningkatan keselamatan yang berterusan	
2.0	Pengurusan Risiko Keselamatan ICT	
	Proses analisis risiko keselamatan ICT disyorkan dilakukan oleh Bahagian ICT Jabatan / Agensi masing-masing. Laporan penilaian hendaklah dimajukan kepada Jawatankuasa Pemandu ICT. Perkara-perkara berikut perlu diambil perhatian dalam melaksanakan analisis risiko : i. Aset-aset ICT (perkakasan, perisian dan maklumat) ii. Sumber manusia (kakitangan, sub-kontraktor	Bahagian ICT Jabatan / Agensi Negeri

	dan lain-lain personel luaran) iii. Persekitaran ICT (bangunan dan kemudahan) iv. Aktiviti-aktiviti ICT (operasi, senggaraan dan pembangunan)	
3.0	Security Posture Assessment (SPA)	
	Melaksanakan program SPA ke atas infrastruktur dan sistem ICT Jabatan / Agensi Negeri sekurang-kurangnya sekali setahun	Bahagian ICT Jabatan / Agensi Negeri

Perkara 04 Klasifikasi Dan Pengendalian Maklumat

1.0	Objektif	Tanggungjawab
	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT	
2.0	Klasifikasi Maklumat	
	Prosedur mengklasifikasikan maklumat yang diuruskan melalui aset ICT hendaklah berpandukan kepada Arahan Keselamatan Kerajaan seperti berikut : i. Rahsia Besar ii. Rahsia iii. Sulit iv. Terhad Ketua Jabatan atau setaraf dipertanggungjawabkan mengeluarkan arahan khas jika perlu untuk dilaksanakan di bahagian masing-masing	Ketua Pegawai Maklumat (CIO)
3.0	Pengendalian Maklumat	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan 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 pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan	Semua

	vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum	
4.0	Inventori Aset	
	Semua aset ICT hendaklah direkodkan. Ini termasuk mengenalpasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya	Pentadbir Sistem ICT
	Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya	Semua

Perkara 05 Keselamatan Sumber Manusia

1.0	Objektif	Tanggungjawab
	Keselamatan sumber manusia adalah penting dan perlu diberi perhatian supaya mereka berupaya menggunakan sistem ICT yang wujud dan tidak memudaratkan sistem tersebut. Ini bertujuan bagi mengurangkan risiko kesilapan manusia, kecuaian, penipuan, kecurian maklumat, pemalsuan identiti dan penyalahgunaan kemudahan	
2.0	Terma Dan Syarat Perkhidmatan	
	Semua kakitangan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa. Semua kakitangan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972	Ketua Jabatan / Ketua Pegawai Maklumat (CIO)
3.0	Menangani Insiden Keselamatan ICT	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera : i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau dideahkan kepada pihak-pihak yang tidak diberi kuasa ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan atau disyaki hilang, dicuri atau didedahkan iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar v. Berlaku cubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.	Semua

4.0	Latihan Kesedaran Keselamatan ICT	
	Program kesedaran keselamatan ICT dilaksanakan kepada semua peringkat kakitangan. Pengguna dan pentadbir komputer perlu menghadiri latihan, memahami dasar dan tatacara penggunaan terutamanya yang melibatkan keselamatan ICT	Pegawai Keselamatan ICT (ICTSO)
5.0	Kejuruteraan Sosial (Social Engineering)	
	Semua kakitangan Jabatan / Agensi Negeri perlu berhati-hati dengan kejuruteraan sosial yang menggunakan pengaruh, pemujukan dan penipuan untuk mendapatkan maklumat daripada manusia. Teknik yang sering digunakan adalah seperti berikut : i. E-mail Phishing ii. Phone Phishing iii. Umpan (Baiting) iv. Interview Phishing Semua kakitangan Jabatan / Agensi Negeri perlu segera memaklumkan kepada ICTSO masing-masing atau CERT negeri bagi mendapatkan pengesahan sekiranya berlaku perkara seperti berikut : i. Menerima sebarang mel elektronik yang meminta pengesahan nombor akaun / id pengguna dan kata laluan atas alasan sesuatu masalah telah berlaku dengan masuk ke laman web khas yang disediakan atau menelefon ke nombor bebas tol yang disediakan ii. Menerima panggilan telefon yang meminta nombor akaun / id pengguna dan kata laluan atas alasan sesuatu masalah berlaku pada akaun tersebut iii. Menjumpai media seperti thumb drive / disket / CD yang mempunyai label kononnya terdapat	Semua

	maklumat sulit kerajaan di dalamnya iv. Menerima kunjungan dari orang yang tidak dikenali yang mengakui pegawai baru / wakil daripada Jabatan / Agensi / Kementerian untuk temuduga atau mendapatkan maklumat sulit. Sekiranya ini berlaku, sila buat panggilan segera ke Jabatan / Agensi / Kementerian berkaitan untuk pengesahan identiti individu tersebut sebelum menjawab sebarang pertanyaan. Sekiranya didapati identiti individu tersebut adalah palsu, sila buat laporan polis	
6.0	Pelanggaran Dasar	
	Pelanggaran Dasar Keselamatan ICT akan dikenakan tindakan tatatertib	Semua

Perkara 06 Keselamatan Fizikal Dan Persekitaran

1.0	Objektif	Tanggungjawab
	Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat	
2.0	Perimeter Keselamatan Fizikal	
	Keselamatan fizikal dan persekitaran adalah merupakan komponen keselamatan ICT yang penting bagi melindungi aset-aset ICT dan maklumat terperingkat daripada diakses secara tidak sah atau dimusnahkan oleh sama ada kerosakan secara fizikal atau individu. Kerosakan fizikal tersebut boleh disebabkan oleh kecuaian individu dan bencana alam seperti kebakaran dan banjir. Terdapat beberapa ancaman terhadap keselamatan fizikal dan persekitaran yang perlu diambil kira seperti berikut : i. Kebakaran ii. Banjir iii. Keupayaan akses secara tidak sah iv. Kehilangan v. Senggaraan vi. Kecuaian vii. Pengawasan Semua ancaman tersebut boleh diatasi dengan kesedaran semua peringkat pengguna sistem ICT menerusi budaya kerja yang cekap mengikut kaedah dan prosedur yang ditetapkan	Pejabat Ketua Pegawai Keselamatan / Pegawai Keselamatan Pejabat, Ketua Pegawai Maklumat (CIO) dan Pegawai Keselamatan ICT (ICTSO)
3.0	Kawalan Fizikal	
	Semua perkakasan, perisian dan peralatan rangkaian komputer hendaklah diletakkan di tempat yang selamat dan terkawal. Penempatan perkakasan komputer mestilah dihindar daripada punca kecuaian dan unsur-unsur sabotaj. Semua kabel rangkaian yang digunakan	Pentadbir Sistem ICT dan Pihak Ketiga

	hendaklah mempunyai salutan (coating) yang tebal dan sukar untuk pecah serta dimasukkan ke dalam saluran paip (conduit) mengikut piawaian antarabangsa dan undang-undang siber negara. Setiap pemasangan kabel rangkaian hendaklah dilabelkan di kedua-dua hujung antara punca dan destinasi kabel tersebut bagi memudahkan proses penjejakan (tracing) apabila berlaku sesuatu insiden keselamatan ICT. Lokasi kritikal yang menyimpan maklumat terperingkat hendaklah diasingkan daripada lokasi yang menyimpan maklumat tidak terperingkat	
4.0	Kawalan Akses Pusat Data / Bilik Server	
4.1	Kawalan akses ke pusat data / bilik server hendaklah ditentukan keselamatannya. Kawalan akses boleh diadakan dalam bentuk seperti berikut : i. Biometrik ii. Kata laluan iii. Sistem elektronik kad pimtar dan mekanikal Semua akses yang dibenarkan ke kawasan persekitaran pusat data / bilik server hendaklah diiringi oleh Pentadbir Pusat Data atau kakitangan teknikal yang dilantik bagi menentukan dan mengawal selia penugasan yang diperlukan. Buku log juga perlu disediakan untuk tujuan merekodkan maklumat dan aktiviti yang dilaksanakan oleh Pentadbir Sistem ICT atau Pihak Ketiga. Sebarang pemindahan maklumat daripada pusat data / bilik server hendaklah dipohon dan mendapat kebenaran daripada pemilik data (data owner) dan Ketua Jabatan masing-masing Bilik Server atau Pusat Data perlu mematuhi ciri-ciri asas seperti berikut:	Semua dan Pihak Ketiga

	a. Suhu tidak melebihi 21 darjah Celcius b. Dipasang dengan Lantai Bertingkat (raised floor) c. Pemasangan kabel yang kemas d. Mempunyai rekod keluar masuk e. Kawalan akses keluar masuk f. Alat pencegah kebakaran dan kelembapan g. Jauh dari ancaman bencana h. SOP pengurusan Pusat Data perlu diwujudkan.	
5.0	Kawalan Persekitaran	
	Bangunan yang menempatkan pusat data / bilik server hendaklah mempunyai kawalan persekitaran seperti berikut : i. Susun atur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi ii. Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelak kerosakan komponen elektronik pada perkakasan berkenaan. Pemeriksaan hendaklah dilaksanakan setiap enam bulan bagi menentukan keberkesanannya iii. Menyediakan sistem pengudaraan (ventilation) yang mencukupi iv. Penggunaan lantai bertingkat (raised floor) dalam pusat data / bilik server v. Penggunaan kamera boleh dilaksanakan bagi meningkatkan kawalan keselamatan Bangunan yang menempatkan pusat data / bilik server hendaklah menentukan ciri-ciri keselamatan seperti berikut : i. Bekalan kuasa elektrik mesti dari punca yang	Semua

	berasingan dan berkemampuan menampung semua beban termasuk server, alat penghawa dingin, alat penggera dan lain-lain ii. ”Centralized Uninterruptable Power Supply” (UPS) dan / atau janakuasa sokongan (back up) hendaklah disediakan dan diuji setiap tiga bulan bagi menentukan bekalan kuasa berterusan iii. Sistem pengaliran air yang sempurna bagi mengelakkan banjir. Pemeriksaan terhadap bangunan yang berkenaan hendaklah dilaksanakan setiap enam bulan oleh penyelia bangunan yang bertauliah atau dilantik	
6.0	Kawalan Perkhidmatan Dan Penyelenggaraan	
	a) Naziran boleh dilaksanakan secara mengejut atau secara berjadual bagi memastikan keselamatan ICT. b) Bangunan yang mempunyai kuasa yang tidak stabil hendaklah dipasang dengan UPS atau ”Automatic Voltage Regulator” (AVR) pada komputer bagi menentukan ketahanan komponen elektronik komputer berkaitan. c) Semua penyelenggaraan terhadap ”Central Processing Unit” (CPU) hendaklah dibuat secara dalaman. Sekiranya perlu dibaiki oleh pihak swasta, cakera keras hendaklah dikeluarkan terlebih dahulu dari CPU setelah mendapat kebenaran pegawai ICT yang bertanggungjawab. d) Penyelenggaraan secara pencegahan (preventive) dan pembetulan (corrective) perlu dirancang secara berjadual bagi menentukan kesinambungan perjalanan sistem berkenaan. Kontrak penyelenggaraan hendaklah disediakan mengikut prosedur semasa.	Semua

	e) Perangkap kilat (lighting arrestor) hendaklah disediakan di semua bangunan penempatan pusat data / bilik server bagi mengelakkan kemasukan kuasa elektrik berlebihan (power surge) yang disebabkan oleh pancaran kilat	
7.0	Kawalan Peralatan	
	a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada Semua kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh	Semua

	Uninterruptable Power Supply (UPS); j) Semua peralatan ICT hendaklah disimpan atau diletakkan ditempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. k) Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; m) Peralatan ICT yang hendak dibawa keluar dari jabatan, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; p) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; q) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; r) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; t) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; u) Pengguna bertanggungjawab terhadap perkakasan,	

	perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; v) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; x) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
8.0	Kawalan Dokumen	
	a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

Perkara 07 Keselamatan Komunikasi Dan Rangkaian

1.0	Objektif	Tanggungjawab
	Bahagian ini adalah tertumpu kepada infrastruktur rangkaian komunikasi iaitu rangkaian internet, intranet dan secured network. Ini juga meliputi aset rangkaian (router, switch, hub, modem dan server), sistem pengkabelan dan segala perkhidmatan pengkomputeran. Ini bertujuan menjaga keselamatan rangkaian dan komunikasi komputer	
2.0	Perancangan Dan Penerimaan Sistem	
	a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawalselia oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. b) Keperluan kapasiti ini juga perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. c) Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan atau dipersetujui	Pentadbir Sistem ICT dan Pegawai Keselamatan ICT (ICTSO)
3.0	Kawalan Perisian	
	a) Pentadbir sistem dikehendaki menentukan penggunaan perisian-perisian daripada sumber-sumber yang sah sahaja. Penggunaan perisian-perisian daripada sumber yang tidak sah dilarang sama sekali bagi mengelakkan sebarang kod malicious tersebar / disebar dalam sistem ICT. b) Perisian-perisian yang berfungsi sebagai audio / video streaming dan peer to peer adalah dilarang sama sekali.	Semua

	c) Setiap komputer dipasang dengan perisian antivirus yang terkini dan patern virus mestilah dikemaskini. d) Untuk mengelak penyebaran atau jangkitan daripada perisian malicious, semua perisian atau sistem mestilah diimbas dengan antivirus dan diperiksa dan disahkan selamat sebelum digunakan. Ia merangkumi juga setiap media storan luar yang dibawa masuk. e) Semua sistem ICT tidak dibenarkan menggunakan perisian yang tidak berlesen kecuali perisian open source yang dibenarkan. 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 yang dibangunkan. i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
4.0	Perlindungan dari Perisian Berbahaya	
	Perkara-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) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;	Pentadbir Sistem/Rangkaian/ Pengguna

	c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini antivirus dengan *pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi semua program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
5.0	Housekeeping	
	a) Salinan penduaan hendaklah dilakukan seperti berikut : i. Salinan direkodkan dan disimpan di off-site. Lokasi off-site tidak boleh di bangunan yang sama dan pemilihan lokasi mestilah praktikal dengan mengambilkira aspek geografi, kemudahan, keselamatan, kos dan persekitaran. ii. Salinan dilakukan secara berkala. iii. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. iv. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. v. Menguji sistem penduaan sedia ada bagi	Pentadbir Sistem

	memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. b) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan.	
6.0	Pengurusan Infrastruktur Rangkaian	
	a) Pengurusan rangkaian Kedah*Net di jabatan-jabatan negeri adalah di bawah penyelarasan PTMK. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi PTMK. b) Pengurusan rangkaian LAN di agensi-agensi negeri adalah di bawah penyelarasan Bahagian ICT masing-masing. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi Bahagian ICT masing-masing. c) Secured Network adalah tidak dibenarkan sama sekali disambungkan dengan sebarang rangkaian awam (Internet). d) Intranet tidak boleh disambungkan kepada rangkaian awam tanpa menggunakan mekanisme keselamatan yang diluluskan oleh Jawatankuasa CERT Negeri. e) Semua jabatan / agensi negeri hendaklah mewujudkan mekanisme untuk memastikan pematuhan terhadap segala arahan keselamatan setiap rangkaian di bawah tanggungjawabnya. f) Penggunaan *administrator tools* dan *hacking tools* tidak dibenarkan dipasang pada komputer pengguna melainkan mendapat kebenaran ICTSO. g) Sebarang pengujian perkakasan dan perisian	Pentadbir Sistem/ ICTSO

	aplikasi sistem hendaklah mendapat kebenaran daripada Pentadbir Sistem. h) Kawalan capaian yang selamat (VPN Connection) hendaklah diwujudkan untuk akses kepada komponen-komponen rangkaian komunikasi. i) Semua konfigurasi dan infrastruktur rangkaian hendaklah diklasifikasikan, didokumenkan dan sentiasa dikemaskini oleh Pentadbir Rangkaian dari semasa ke semasa. j) Kawalan Server secara jarak jauh (remote access) boleh dipertimbangkan di dalam pengurusan Pusat Data setelah mengambil kira faktor kawalan keselamatan. Kawalan akses ini perlu dipatuhi melalui SOP yang menyenaraikan aspek kawalan keselamatan iaitu penggunaan kata laluan yang selamat, tapisan MAC ADDRESS dan/atau Routing. k) Capaian ke Internet dan sistem yang terletak di dalam *Secured Network* yang melalui infrastruktur rangkaian awam hendaklah mempunyai ciri-ciri keselamatan tambahan. l) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam PKPA Bil 1 Tahun 2003 atau pekeliling-pekeliling terkini.	
7.0	Pengurusan Media	
	a) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. b) Mematuhi prosedur pengendalian media seperti berikut : i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. ii. Menghadkan dan menentukan capaian media	Semua

	kepada pengguna yang sah sahaja. iii. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan. iv. Menyimpan dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. v. Menyimpan semua media di tempat yang selamat. vi. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.	
8.0	Keselamatan Komunikasi	
8.1	Perkhidmatan Mel Elektronik (e-Mel)	
	a) Bahagian ini merujuk dan menggunapakai arahan yang terkandung di dalam Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003. b) Pentadbir Sistem mesti memastikan setiap pelayan e-Mel dipasang dengan pelayan antivirus e-Mel bagi membolehkan pengimbasan dilakukan sebelum e-Mel sampai kepada pengguna. c) Penggunaan kemudahan ini adalah untuk tujuan perkhidmatan rasmi sahaja. d) Semua pihak bertanggungjawab sepenuhnya terhadap semua kandungan e-Mel di dalam akaun sendiri. e) Kelayakan kakitangan untuk mendapat akaun e-Mel sesuai dengan jawatan dan mengikut polisi semasa. Sebarang perubahan status penggunaan (bertukar keluar atau berhenti) hendaklah dimaklumkan kepada Pentadbir Sistem e-Mel. f) Penghantaran maklumat terperingkat melalui Internet mestilah menggunakan kaedah penyulitan	Semua dan Pentadbir Sistem ICT

	yang dibenarkan. g) Sebarang penggunaan e-Mel yang boleh memudaratkan nama baik jabatan / agensi serta Kerajaan Negeri Kedah adalah dilarang sama sekali. h) Komunikasi e-Mel bagi tujuan rasmi mestilah menggunakan akaun e-Mel rasmi kerajaan sahaja. i) Kenyataan Penafian (Disclaimer) perlu diletakkan di dalam setiap e-Mel rasmi kerajaan seperti : This email, including any attachments, is confidential and for use only by intended recipient(s) for the purpose for which it has been sent. Its contents may be privileged and if you are not the intended recipient of this email, you must not use, disseminate, print or copy this email or any part of it or take any action in reliance on it. If you have received this email in error, please contact the sender immediately by return email or telephone and delete/destroy the message. We do not accept liability for any corruption, delay, interception or unauthorized amendment of the e-mail or their consequences. j) Segala akaun e-Mel yang diberi adalah bukan hak persendirian. Pentadbir Sistem e-Mel berhak mengakses mana-mana akaun bagi tujuan pengurusan akaun e-Mel, keselamatan dan undang-undang. k) Elakkan dari membuka e-Mel daripada penghantar yang tidak diketahui dan diragui. l) Mengimbas bahan-bahan yang hendak dimuat naik atau dimuat turun supaya bebas virus sebelum digunakan. m) Setiap lampiran maklumat yang sulit perlu melalui proses enkripsi sebelum penghantaran secara elektronik dilakukan. Ini adalah bagi mengelak kemungkinan maklumat tersebut dipintas oleh individu yang tidak bertanggungjawab. n) Semua pihak dilarang daripada melakukan aktiviti	Semua dan Pentadbir Sistem ICT

	yang melanggar tatacara penggunaan e-Mel rasmi kerajaan seperti : i. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain. ii. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah. iii. Menggunakan e-Mel bagi tujuan peribadi (bukan rasmi), komersial atau politik. iv. Menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah. v. Menghantar dan melibatkan diri dalam e-Mel yang berunsur hasutan, e-Mel sampah, e-Mel bom, e-Mel spam, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Negeri dan Kerajaan Malaysia. vi. Menyebarkan kod perosak seperti virus, worm, trojan dan trap door yang boleh merosakkan sistem komputer dan maklumat pengguna lain. vii. Menghantar semula e-Mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian. viii. Membenarkan pihak ketiga untuk menjawab e-Mel kepada penghantar asal bagi pihaknya.	
8.2	Perkhidmatan Melayari Internet	
	a) Bahagian ini merujuk dan menggunapakai arahan yang terkandung di dalam Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003. b) Semua pihak dikehendaki menyediakan kawalan terhadap penggunaan kemudahan Internet. c) Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan.	Semua dan Pentadbir Sistem ICT

	d) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan. e) Kemudahan ini disediakan untuk tujuan capaian hal yang bersangkutan dengan perkhidmatan dan dibenarkan untuk tujuan-tujuan produktif. f) Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik. g) Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Ketua Jabatan sahaja. h) Semua pihak dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti : i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen. ii. Menyedia dan menghantar maklumat berulang-ulang berupa gangguan. iii. Melayari, menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah. iv. Melayari, menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej kerajaan. v. Menyalahguna kemudahan perbincangan awam dan jaringan sosial atas talian seperti newsgroup,	Semua dan Pentadbir Sistem ICT

	bulletin board, facebook, twitter dan sebagainya. vi. Memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain. vii. Melayari, memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti perjudian, permainan elektronik, video dan lagu. viii. Menggunakan kemudahan chatting melalui Internet dalam hal yang tidak berkaitan dengan urusan kerja. ix. Memuat turun, menyimpan dan menggunakan perisian *peer to peer*. x. Menggunakan kemudahan Internet untuk tujuan peribadi. xi. Menjalankan aktiviti-aktiviti komersial dan politik. xii. Melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas. xiii. Menggunakan sebarang perkakasan yang berfungsi sebagai modem ke atas komputer dalam rangkaian kerajaan untuk membuat capaian terus ke Internet. i) Komputer peribadi yang digunakan untuk mencapai Internet mesti dilengkapi dengan ciri-ciri keselamatan tambahan seperti perisian antivirus dan *anti-spyware*.	Semua dan Pentadbir Sistem ICT
8.3	Perkhidmatan Laman Web	
	a) Notis hakcipta perlu diletakkan pada semua laman web rasmi seperti : ”Hakcipta Portal Rasmi (nama Agensi) dan kandungannya yang termasuk maklumat, teks, imej, grafik, fail suara, fail video dan susunannya serta bahan-bahannya ialah kepunyaan (nama	Semua dan Pentadbir Sistem ICT

	agensi) kecuali dinyatakan sebaliknya. Tiada mana-mana bahagian portal ini boleh diubah, disalin, diedar, dihantar semula, disiarkan, dipamerkan, diterbitkan, dilesenkan, dipindah, dijual atau diuruskan bagi tujuan komersial dalam apa bentuk sekalipun tanpa mendapat kebenaran secara bertulis yang jelas terlebih dahulu daripada (nama agensi). Produk-produk lain, logo dan syarikat atau organisasi yang tercatat di dalam portal ini adalah kepunyaan syarikat atau organisasi tersebut." b) Kenyataan Penafian (Disclaimer) perlu diletakkan pada semua laman web rasmi seperti : "Kerajaan Malaysia dan (nama agensi) adalah tidak bertanggungjawab bagi apa-apa kehilangan atau kerugian yang disebabkan oleh penggunaan mana-mana maklumat yang diperolehi dari portal ini serta tidak boleh ditafsirkan sebagai ejen kepada, ataupun syarikat yang disyorkan oleh (nama agensi)." c) Dasar Privasi dan Keselamatan perlu diletakkan pada semua laman web rasmi seperti : "Halaman ini menerangkan dasar privasi yang merangkumi penggunaan dan perlindungan maklumat yang dikemukakan oleh pengunjung. Sekiranya anda membuat transaksi atau menghantar e-mel mengandungi maklumat peribadi, maklumat ini mungkin akan dikongsi bersama dengan agensi awam lain untuk membantu penyediaan perkhidmatan yang lebih berkesan dan efektif. Contohnya seperti di dalam menyelesaikan aduan yang memerlukan maklumbalas dari agensi-agensi lain."	
9.0	Pemantauan	
9.1	Pengauditan dan Forensik ICT	
	ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT Kerajaan Negeri Kedah; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal	

	(*physical loss*); 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 jalur lebar (*bandwidth*) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO
9.2	Jejak Audit	
	Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; d) Maklumat aktiviti sistem yang tidak normal atau	Pentadbir Sistem ICT

	aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
9.3	Sistem Log	
	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara 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; c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
9.4	Pemantauan Log	
	Perkara-perkara yang perlu dipatuhi adalah 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	Pentadbir Sistem ICT

	memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; f) Waktu yang berkaitan dengan sistem pemprosesan maklumat atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
10.0	Lain-Lain Perkhidmatan	
	Lain-lain perkhidmatan atau utiliti yang mempunyai risiko terhadap pendedahan maklumat rasmi jabatan /agensi negeri serta Kerajaan Negeri Kedah dan keselamatan ICT secara langsung atau tidak langsung adalah dilarang tanpa kebenaran CIO dan / atau ICTSO	

Perkara 08 Kawalan Capaian

1.0	Objektif	Tanggungjawab
	Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT	
2.0	Akaun Pengguna	
	a) Semua pengguna sistem ICT mestilah mempunyai ID pengguna (user ID) dan kata laluan (password) masing-masing dan bertanggungjawab terhadapnya. b) Penggunaan teknologi tambahan seperti kad-kad pintar dan teknologi *biometric authentication* perlu dipertimbangkan untuk sistem yang terperingkat. c) Pengguna disarankan mengadakan kemudahan password screen saver atau log off sekiranya meninggalkan komputer. d) ID pengguna dan kata laluan tidak boleh dikongsi. e) Kata laluan mesti sekurang-kurangnya lapan aksara dan mempunyai kombinasi huruf, nombor dan aksara khas. f) Kata laluan perlu ditukar sekurang-kurangnya setiap tiga (3) bulan sekali. g) Pemilikan akaun pengguna bukanlah hak milik mutlak seseorang dan ia tertakluk kepada peraturan jabatan / agensi. Akaun boleh ditarik balik jika penggunanya melanggar peraturan. h) Akaun pengguna akan ditamatkan atas sebab-sebab seperti berikut : i. Bersara ii. Ditamatkan perkhidmatan iii. Bertukar ke jabatan / agensi lain iv. Bertukar bidang tugas kerja v. Menyalahguna kemudahan akaun ICT yang diberikan	Semua

	i) Akaun pengguna disaran dibekukan sepanjang tempoh pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh melebihi sebulan. j) Semua akses kepada aset ICT hendaklah ditentukan dan didokumenkan melalui prosedur pendaftaran pengguna dan dikawal berdasarkan kepada prinsip perlu mengetahui, peranan, hak akses minimum dan pengasingan tugas. Semua hak keistimewaan dan akses hendaklah dikaji semula secara berkala. Akses yang mempunyai hak keistimewaan hendaklah dihadkan dan dipantau oleh Pegawai Keselamatan ICT. Aktiviti akses hendaklah dipantau untuk mengesan aktiviti luar biasa seperti cubaan berulang akses yang tidak sah yang mungkin mengancam integriti, kerahsiaan atau ketersediaan sistem.	
3.0	Kawalan Akses	
	Setiap keperluan akses mestilah dirancang dan didokumentasikan berdasarkan kawalan akses dan klasifikasi maklumat. Pengguna mestilah dimaklumkan mengenai tahap akses yang ditetapkan	Pemilik Sistem dan Pentadbir Sistem ICT
4.0	Perakaunan Dan Jejak Audit (Audit Trail)	
	a) Semua perkakasan / utiliti mestilah mengaktifkan audit log. Audit log perlu disimpan sekurang-kurangnya dalam tempoh setahun sebelum dilupuskan. b) Semua laporan log / audit trail dan program atau utiliti mestilah dikawal dan hanya boleh diakses oleh Pentadbir Sistem dan personel keselamatan sahaja. c) Aktiviti-aktiviti Pentadbir Sistem mestilah dilogkan. d) Sebarang cubaan memasuki sistem (login) yang tidak berjaya mestilah dilogkan dan perlu diberi	Pemilik Sistem dan Pentadbir Sistem ICT

	perhatian. e) Penggera keselamatan boleh dipertimbangkan untuk memberikan amaran kepada Pentadbir Sistem secara automatik sebagai tanda peringatan. f) Pentadbir Sistem dan Pentadbir Rangkaian dikehendaki menganalisa log / audit trail sekurang-kurangnya sekali dalam seminggu. g) Semua sistem komputer dan peranti rangkaian mestilah mempunyai catatan masa yang seragam bagi memastikan kesahihan masa yang tercatat dalam audit log. Pentadbir Sistem harus menentukan penyatuan masa sekurang-kurangnya sekali dalam sebulan.	
5.0	Kawalan Capaian Sistem Maklumat Dan Aplikasi	
	a) Capaian sistem dan aplikasi adalah terhad kepada pengguna dan tujuan yang dibenarkan. b) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan. c) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. d) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dan sebarang bentuk penyalahgunaan. e) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. f) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	Pentadbir Sistem ICT dan ICTSO

6.0	*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* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
7.0	Kawalan Capaian Rangkaian	
7.1	Capaian Rangkaian	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Kedah*Net, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO
7.2	Capaian Internet	
	Perkara-perkara yang perlu dipatuhi adalah seperti	

	berikut: a) Penggunaan Internet 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; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa; f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;	Pentadbir Rangkaian Pengurus ICT Semua

	i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan; j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; l) 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, lagu yang boleh menjejaskan tahap capaian internet; ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
8.0	Kawalan Capaian Sistem Pengoperasian	
8.1	Capaian Sistem Pengoperasian	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Merekodkan capaian yang berjaya dan gagal.	Pentadbir Sistem ICT dan ICTSO

	Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user;* c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti 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; c) Menghadkan dan mengawal penggunaan program; d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
8.2	Kad Pintar	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 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;	Semua

	d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Pentadbiran.	
9.0	Keselamatan Komputer Mudah Alih / Riba	
	a) Instalasi perisian komputer mudah alih mestilah dilaksanakan oleh kakitangan ICT. b) Komputer mudah alih hendaklah sentiasa di bawah penjagaan yang rapi bagi menjamin keselamatannya dari kecurian dan kerosakan. c) Pengguna yang membawa maklumat terperingkat dikehendaki mengisytiharkannya dengan mendapat kebenaran bertulis dari Ketua Jabatan atau setaraf. d) Pengguna yang menggunakan komputer mudah alih persendirian untuk tugas perkhidmatan mestilah mendapat kelulusan bertulis daripada Ketua Jabatan dan setaraf serta tertakluk kepada tindakan, pengawasan dan pemantauan bahagian ICT jabatan / agensi yang berkaitan. e) ICTSO dengan bantuan bahagian ICT jabatan / agensi yang berkaitan mempunyai hak untuk membuat sebarang proses penghapusan atau pemindahan sebarang maklumat jabatan daripada pegawai yang menggunakan komputer riba persendirian sekiranya pegawai tersebut berpindah, bersara atau diberhentikan perkhidmatannya.	Semua
10.0	Aset ICT	
	Semua aset ICT mesti dijaga dengan rapi bagi menjamin keselamatannya dari kecurian atau kerosakan dan perlu mendapat kebenaran bertulis daripada Ketua Jabatan untuk dibawa keluar sekiranya ada maklumat terperingkat	

Perkara 09 Keselamatan Sistem Aplikasi

1.0	Objektif	Tanggungjawab
	Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian	
2.0	Keselamatan Dalam Membangunkan Sistem Dan Aplikasi	
	a) Pembangunan 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 : i. Sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan. ii. Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna. iii. Sistem output untuk memastikan data yang telah diproses adalah tepat. 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. d) Pembangunan Sistem aplikasi yang berasaskan kepada Open Source adalah digalakkan. Walau bagaimanapun, ianya perlu memenuhi pertimbangan seperti berikut : 1. Mesti bersesuaian dengan tujuan dari segi fungsi dan juga platform teknologi. 2. Tidak memberi gangguan kepada operasi urusan sedia ada. 3. Mesti ada keupayaan untuk wujud bersama-sama sistem legasi lain.	Pemilik Sistem, Pentadbir Sistem ICT

	e) Keselamatan bagi aplikasi hendaklah mempunyai ciri-ciri berikut : -Logoff secara automatic apabila tiada aktiviti dalam tempoh yang ditetapkan. -Pengesahan semula pengguna yang aktif secara automatic selepas tempoh yang ditetapkan. - Tidak membenarkan lebih dari satu sesi *login* untuk setiap pengenalan pengguna - Wujud pengenalan pengguna yang unik dalam sistem; -Hentikan akaun pengguna selepas maksimum tiga (3) kali gagal cubaan *login*; -Gantung hak keistimewaan pengguna selepas 30 hari (boleh diubah) sekiranya tidak digunakan dan menghapuskannya selepas 30 hari (boleh diubah) digantung penggunaan; -Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; -Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula; -Kuatkuasakan penggunaan kata laluan minimum 8 aksara dengan kombinasi aksara, angka dan aksara khas. - Cegah penggunaan semula empat (4) kata laluan yang terakhir digunakan.Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; -Tentukan had masa pengesahan selama dua (2) minit (boleh diubah) dan selepas had itu, sesi ditamatkan; dan -Papar tarikh dan masa terakhir *login* pengguna yang berjaya dan yang tidak berjaya.	
3.0	Pengesahan Data Input Dan Output	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem

	a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat. c) Data yang dimasukkan ke dalam sistem aplikasi mesti disemak bagi memastikan kesahihan. Mekanisma semakan seperti Standard Operating Prosedures (SOP) perlu disedia dan diperakui oleh pengurusan jabatan/agensi.	
4.0	Kriptografi (Cryptography)	
	a) Maklumat terperingkat atau maklumat rahsia rasmi hendaklah melalui proses penyulitan (encryption) setiap masa sebelum dihantar atau disalurkan ke dalam sistem rangkaian yang tidak selamat seperti Internet, Mobil-GSM, Infrared dan sebagainya. b) Penggunaan tandatangan digital adalah disyorkan kepada semua pengguna khususnya mereka yang menguruskan transaksi atau maklumat rahsia rasmi setiap masa. c) Pengurusan kunci penyulitan hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
5.0	Kawalan Fail Sistem	
	a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. b) Mengawal capaian ke atas kod aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. c) Mengaktifkan audit log bagi merekodkan semua	Pentadbir Sistem ICT

	pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
6.0	Pembangunan Dan Proses Sokongan	
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai	Pentadbir Sistem ICT
7.0	Kawalan Teknikal Keterdedahan (*Vulnerability*)	
7.1	Kawalan dari Ancaman Teknikal	
	Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT
8.0	Penetapan Time-Synchronization	
	Prosedur bagi menyemak ketepatan jam dan pembetulan mesti diwujudkan seperti menggunakan Network Time Protocol (NTP) yang direka bentuk untuk menyelaraskan jam sistem komputer dan pelayan (URL : http://www.ntp.org). Real-time clock bagi peranti komunikasi mesti ditetapkan mengikut “Malaysian Standard Time Act 1981”. Semua sistem aplikasi dan pelayan menggunakan “ Malaysian Standard Time”.	Pentadbir Sistem
9.0	Ujian Penembusan	
	Semua sistem ICT perlu menjalani proses Penilaian Tahap Keselamatan Rangkaian dan Sistem Aplikasi sebelum digunakan secara rasmi oleh jabatan/agensi. Ujian Penembusan (pentest) perlu dilakukan bagi	ICTSO

	mengetahui tahap risiko atau kelemahan skrip/konfigurasi.	
10.0	Fail Backup	
	Fail *backup* hendaklah dilabelkan dengan teratur dan jelas untuk mengelakkan kesilapan *overwrite* secara tidak sengaja. Kawalan akses terhadap fail *backup* hendaklah dihadkan kepada personel yang diizinkan dengan rekod pengauditan yang teratur. Kekerapan *backup* bergantung kepada tahap kritikal maklumat. Media *backup* hendaklah disimpan dengan selamat dan di premis luar. Akses kepada lokasi storan yang dilindungi hendaklah dikawal dengan ketat daripada akses tanpa izin. Agensi hendaklah menguji prosedur *backup/pemulihan* dan media *backup* sekurang-kurangnya sekali setahun.	Pentadbir Sistem

Perkara 10 Pelan Kesinambungan Perkhidmatan Dan Pemulihan Bencana

1.0	Objektif	Tanggungjawab
	Semua perkhidmatan yang berasaskan ICT terutama proses-proses kritikal perlu disediakan pelan kesinambungan perkhidmatan. Pelan tersebut hendaklah dipastikan boleh digunapakai apabila diperlukan. Ia bertujuan memastikan operasi-operasi di jabatan / agensi negeri berjalan secara berterusan ketika berlaku gangguan atau bencana	
2.0	Pelaksanaan	
	a) Business Continuity Management Organisation (BCMO) perlu diwujudkan bagi setiap perkhidmatan kritikal / berisiko tinggi yang berasaskan ICT. BCMO terdiri daripada : i. Jawatankuasa Pemandu Pengurusan Pemulihan Bencana (Business Continuity Steering Committee – BCSC) ii. Kumpulan Pengurusan Kesinambungan Urusniaga (Business Continuity Management Group – BCMG) iii. Kumpulan Pengurusan Pemulihan Urusniaga (Business Recovery Management Group – BRMG) b) Semua Ketua Jabatan dan setaraf hendaklah bertanggungjawab menyediakan pelan Business Continuity Planning (BCP) yang lengkap dan jelas. c) Pelan ini hendaklah dibentang dan dipersetujui terima oleh BCSC berkaitan serta diluluskan oleh Jawatankuasa Pemandu ICT. d) Pelan BCP perlu diuji dan disemak sekurang-kurangnya setahun sekali.	Ketua Jabatan Dan ICTSO

Perkara 11 Pematuhan

1.0	Objektif	Tanggungjawab
	Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT	
2.0	Pematuhan Dasar	
	a) Setiap pengguna jabatan / agensi negeri hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT serta undang-undang atau peraturan-peraturan lain yang berkaitan yang telah berkuatkuasa. b) Semua aset ICT termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
3.0	Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
3.1	Pematuhan Keperluan Audit	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan	Semua

	dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
4.0	Keperluan Perundangan Dan Peraturan	
	Berikut adalah keperluan perundangan dan peraturan-peraturan lain yang berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan / agensi negeri : a) Arahan Keselamatan. b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk ”Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”. c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS). 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 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. g) Akta Tandatangan Digital 1997 h) Akta Jenayah Komputer 1997 i) Akta Hak Cipta (Pindaan) Tahun 1997 j) Akta Komunikasi dan Multimedia 1998	Semua

RUJUKAN

1. ”Dasar Keselamatan ICT”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2006
2. ”Malaysian Public Sector ICT Security Risk Assessment Methodology”, Surat Pekeliling Am Bilangan 6, Jabatan Perdana Menteri, 2005
3. “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan“, Pekeliling Am Bilangan 1, Jabatan Perdana Menteri, 2003
4. “Dasar Keselamatan ICT”, Bahagian Teknologi Maklumat, Kementerian Pertahanan Malaysia, 2002
5. ”Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”, Pekeliling Am Bilangan 1, Jabatan Perdana Menteri, 2001
6. ”Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan”, Pekeliling Am Bilangan 3, Jabatan Perdana Menteri, 2000
7. Arahan Keselamatan Malaysia
8. ”Dasar Keselamatan ICT”, Bahagian Teknologi Maklumat, Kementerian Kesihatan Malaysia, 2007
9. Arahan Teknologi Maklumat, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2007
10. ”Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2006
11. ”Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2002
12. “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan“, Pekeliling Kemajuan dan Pentadbiran Am, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 2003
13. SIRIM, MS ISO / IEC 27001 Information Security Management System Standard Malaysia, 2006

14. ”Dasar Keselamatan ICT”, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, Versi 5.3 Mei 2010