DASAR KESELAMATAN ICT NEGERI PULAU PINANG

VERSI 0.0

15 Januari 2009

Dasar Keselamatan ICT Negeri ini telah dibentangkan dan diluluskan oleh Jawatankuasa *Electronic Good Governance* (eGG) pada 15 Januari 2009.

DATO' JAMALUDIN BIN HASAN

Setiausaha Kerajaan Negeri

Pulau Pinang

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 processor, hard disk, memori 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 Sistem (IDS)	Satu peralatan yang digunakan untuk memantau atau merekod cubaan pencerobohan.
Internet	Perkhidmatan informasi secara global yang menghubungkan semua pengguna seluruh dunia melalui satu protokol rangkaian.

Information Security	Proses dan mekanisme untuk melindungi maklumat.
Jawatankuasa Pemandu *Electronic Good Governance (eGG)*	Jawatankuasa ICT Tertinggi di peringkat Kerajaan Negeri Pulau Pinang 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 pun 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 sistem operasi.
Pusat Teknologi Maklumat dan Komunikasi Negeri (PTMKN)	Pusat Teknologi Maklumat dan Komunikasi Negeri (PTMKN) adalah satu bahagian di bawah Pejabat Setiausaha Kerajaan Negeri Pulau Pinang 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 menngenalpasti kelemahan-kelemahan yang terdapat dalam sistem yang boleh memberi ancaman kepada keselamatan sistem.
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.
VPN (Virtual Private Network)	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.

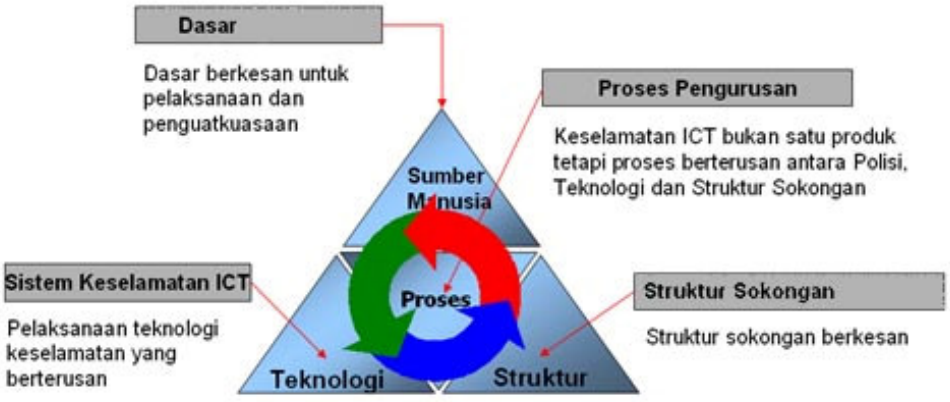
Kandungan

PENDAHULUAN

Kesan penggunaan ICT telah mengubah budaya kerja organisasi. Sementara berbangga dengan kemajuan yang dicapai, semua warga Kerajaan Negeri Pulau Pinang juga perlu peka terhadap isu keselamatan ICT terutama dari segi peranan, tanggungjawab dan kawalan penggunaan. 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 platfom 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. Kepentingan dasar keselamatan ICT boleh digambarkan seperti di ***Rajah 1.***



Rajah 1 : Pelaksanaan Keselamatan ICT

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), 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.

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 setahun[1]. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian apabila diperlukan. Ketua jabatan dan setaraf perlu 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 sokongan *(backup)* setiap hari bagi sistem ICT.

[1] MAMPU, *Arahan Teknologi Maklumat*: Jabatan Perdana Menteri, 2007.

iii. Semua pengguna dikehendaki mencegah kemasukan virus, mengamalkan langkah-langkah pencegahan kebakaran dan amalan *clear desk* mengikut arahan semasa jabatan masing-masing.

f. Pematuhan

Pematuhan Dasar Keselamatan ICT adalah berdasarkan tindakan berikut:

1. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.
2. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
3. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. PTMKN/ Unit ICT Agensi Negeri berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan Negeri/ Agensi berkaitan.
4. Menguatkuasakan amalan melapor sebarang insiden yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan/ pemulihan.

g. Pengasingan

Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi juga hendaklah dilakukan di antara pentadbir sistem dan pentadbir rangkaian.

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 *authentication* 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 dan 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 dan 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.

Perkara 01 Pembangunan dan Penyelenggaraan Dasar

1.0	**Pelaksanaan Dasar**	**Tanggungjawab**
	Pelaksanaan Dasar ini dijalankan oleh Setiausaha Kerajaan Negeri dibantu oleh Jawatankuasa Pemandu *Electronic Good Governence* yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan.	Setiausaha Kerajaan Negeri
	Penyebaran Dasar	
	Dasar ini perlu disebarkan kepada semua pengguna Jabatan/ Agensi Negeri (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
	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 Negeri : a. Kenalpasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO masing-masing untuk dibentangkan kepada Jawatankuasa CERT Negeri bagi mendapatkan persetujuan Mesyuarat Jawatankuasa Pemandu *Electronic Good Governence (eGG)*; c. Perubahan yang telah dipersetujui oleh eGG dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	ICTSO
	Pengecualian Dasar	
	Dasar Keselamatan ICT Negeri adalah terpakai kepada semua pengguna ICT Jabatan / Agensi Negeri dan tiada pengecualian diberikan.	Semua

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. Struktur Organisasi Keselamatan ICT Negeri adalah seperti di **Lampiran A**.	
2.0	**Setiausaha Kerajaan Negeri**	
	Peranan dan tanggungjawab adalah seperti berikut : a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Negeri; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Negeri; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. 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 : a. Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT ; c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; d. Memastikan setiap pegawai dan kakitangan menandatangani surat akuan mematuhi Dasar Keselamatan ICT; e. Mengambil tindakan tatatertib ke atas anggota yang melanggar Dasar Keselamatan ICT Negeri. f. Menguruskan tindakan ke atas insiden keselamatan yang berlaku sehingga keadaan pulih;	Ketua Pegawai Maklumat

	g. Mengaktifkan *Business Resumption Plan* (BRP) jika perlu;dan h. 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: a. Mengurus program-program keselamatan ICT; b. Menguatkuasakan Dasar Keselamatan ICT; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua pengguna; d. Melaksanakan garis panduan, prosedur dan tatacara yang berkaitan selaras dengan keperluan Dasar Keselamatan ICT Negeri; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Menentukan tahap keutamaan insiden, melaporkan insiden keselamatan ICT kepada Pasukan CERT NEGERI dan memaklumkan kepada CIO serta mengambil langkah pemulihan awal; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan langkah-langkah baik pulih dengan segera; j. Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Negeri; dan k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	Pegawai Keselamatan ICT

6.0	**Pentadbir Sistem ICT**	
	Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT; c. Memantau aktiviti capaian harian pengguna; d. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; e. Menyimpan dan menganalisis rekod *audit trail*; dan f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	Pentadbir Sistem ICT
7.0	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dan tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat; d. 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 katalaluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;	Semua

	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. e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan g. Menandatangani surat akuan mematuhi Dasar Keselamatan ICT	
8.0	**Keperluan Keselamatan dengan Pihak Ketiga**	
	Pihak ketiga perlu menandatangani dokumen-dokumen berikut bagi melindungi aset ICT Kerajaan : a. Surat akuan mematuhi Dasar Keselamatan ICT ; dan b. Perakuan Akta Rahsia Rasmi 1972 Kandungan perjanjian kontrak dengan pihak ketiga perlu merangkumi perkara-perkara berikut : c. Dasar Keselamatan ICT d. Perakuan Akta Rahsia Rasmi 1972; dan e. Hak Harta Intelek Penggunaan *Outsourcing* perlu dikawal daripada segi perlaksanaannya bagi menjamin keselamatan terhadap sistem yang akan dilaksanakan secara *outsource.* Kaedah pelaksanaan outsourcing adalah berdasarkan kepada Garis Panduan IT *Outsource* Agensi-Agensi Sektor Awam.	Semua
10.0	**Jawatankuasa Pemandu Keselamatan ICT/ Jawatankuasa Pemandu *Electronic Good Governance***	
	Keahlian dan bidang rujukan Jawatankuasa ini dilaksanakan dibawah Jawatankuasa Pemandu *Electronic Good Governance* (*eGG*). Tugas dan Tanggungjawab khusus berkaitan dengan aspek keselamatan	J/kuasa Pemandu eGG

	ICT adalah seperti berikut : a. Merangka dasar, hala tuju, garis panduan dan piawaian keselamatan ICT. b. Meneliti, meluluskan dan menguatkuasakan dasar keselamatan ICT. c. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT. d. Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan. e. Meluluskan inisiatif untuk peningkatan keselamatan ICT. f. Memantau ancaman-ancaman utama terhadap aset-aset ICT. g. Memastikan pengauditan sistem ICT dilaksanakan sekurang-kurangnya sekali setahun.	
11.0	**Jawatankuasa CERT Negeri**	
	Skop tanggungjawab CERT Negeri merangkumi semua Jabatan Negeri di Pulau Pinang termasuk MAIPP dan Lembaga Muzium Negeri. Keahlian Jawatankuasa ini adalah seperti berikut : a. Pengurus PTMKN – Pengerusi b. Pegawai Teknologi Maklumat (Kanan) Unit Keselamatan dan Pangkalan Data PTMKN c. Pegawai Teknologi Maklumat, Unit Rangkaian, Operasi dan Sokongan Teknikal PTMKN d. Wakil JKN e. Wakil PTG f. Wakil JAIPP g. Wakil PEGIS h. Wakil PDT seluruh Pulau Pinang i. Urusetia -PTMKN Tugas dan tanggungjawab Jawatankuasa ini adalah seperti berikut: a. Menilai aspek-aspek teknikal berhubung inisiatif dan projek keselamatan ICT.	J/kuasa CERT Negeri

	b. Memberi nasihat teknikal kepada Jawatankuasa Pemandu *eGG*. c. Menyediakan pelan tindakan untuk pembangunan dan peningkatan keselamatan sistem ICT. d. Menilai pilihan teknologi dan cadangan penyelesaian terhadap keperluan keselamatan sistem ICT. e. Mengkaji semula dasar keselamatan ICT dari semasa ke semasa untuk dibentangkan kepada JK Pemandu *eGG*.	
	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 J/kuasa CERT Agensi

Perkara 03 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**	
	a. Proses analisis risiko keselamatan ICT disyorkan dilakukan oleh Bahagian ICT masing-masing. Laporan penilaian hendaklah dimajukan kepada Jawatankuasa Pemandu *eGG*. Perkara-perkara berikut perlu diambil perhatian dalam melaksanakan analisis risiko: i. Aset-aset ICT (perkakasan, perisian dan maklumat) ii. Sumber Manusia (kakitangan, sub-kontraktor dan lain-lain personel luaran). iii. Persekitaran ICT (bangunan dan kemudahan) iv. Aktiviti-aktiviti ICT (operasi, senggaraan dan pembangunan)	Bahagian ICT Jabatan/ Agensi Negeri
3.0	***Security Posture Assessment (SPA)***	
	Melaksanakan program SPA ke atas infrastruktur dan sistem ICT Jabatan/Agensi Negeri sekurang-kurangnya satu (1) tahun sekali.	Bahagian ICT Jabatan/ Agensi Negeri

Perkara 04 Pengelasan 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 : a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad. Ketua Jabatan atau setaraf dipertanggungjawabkan mengeluarkan Arahan Khas jika perlu untuk dilaksanakan di bahagian masing-masing.	CIO
3.0	**Pengendalian Maklumat**	
	Aktiviti pengendalian makumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah 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 pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

4.0	**Inventori Aset**	
	a. 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
	b. 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**	
	a. Semua kakitangan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa. b. Semua kakitangan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Ketua Jabatan/ CIO
3.0	**Menangani 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 diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.	Semua

4.0	**Latihan Kesedaran Keselamatan ICT**	
	a. Program kesedaran keselamatan ICT dilaksanakan kepada semua peringkat kakitangan. b. Pengguna dan pentadbir komputer perlu menghadiri latihan, memahami dasar dan tatacara penggunaan terutamanya yang melibatkan keselamatan ICT.	ICTSO
5.0	**Kejuruteraan Sosial (Sosial Engineering)**	
	Kesemua 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 : a. Emel Phishing b. Phone Phishing c. Umpan (Baiting) d. Interview Phishing Kesemua kakitangan Jabatan/ Agensi Negeri perlu segera memaklumkan kepada ICTSO masing-masing atau Pusat Teknologi Maklumat dan Komunikasi Negeri bagi mendapatkan pengesahan sekiranya berlaku perkara seperti berikut : a. Menerima sebarang emel yang meminta pengesahan no. akaun/ id pengguna dan katalaluan atas alasan sesuatu masalah telah berlaku dengan masuk ke laman web khas yang disediakan atau telefon ke nombor tol free yang disediakan. b. Menerima panggilan telefon yang meminta no. akaun/ id pengguna dan katalaluan atas alasan sesuatu masalah berlaku pada akaun tersebut. c. Menjumpai media seperti thumb drive/ disket / CD yang mempunyai label yang kononnya terdapat maklumat sulit kerajaan di dalamnya. d. Menerima kunjungan dari orang yang tidak dikenali yang mengakui pegawai baru/ wakil daripada Jabatan/Agensi/	Semua

	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 indentiti individu tersebut adalah palsu, sila buat laporan polis.	
6.0	**Perlanggaraan 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: a. Kebakaran b. Banjir c. Keupayaan akses secara tidak sah d. Kehilangan e. Senggaraan f. Kecuaian g. 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, CIO dan ICTSO
3.0	**Kawalan Fizikal**	
	a. Semua perkakasan, perisian dan peralatan rangkaian komputer hendaklah diletakkan di tempat yang selamat dan terkawal. b. Penempatan perkakasan komputer mestilah dihindar daripada punca kecuaian dan unsur-unsur sabotaj. c. Semua kabel rangkaian yang digunakan hendaklah mempunyai salutan *(coating)* yang tebal dan sukar untuk pecah serta dimasukkan ke dalam saluran paip *(Conduit)* mengikut piawaian	Pentadbir Sistem ICT dan Pihak Ketiga

	antarabangsa dan undang-undang siber negara. d. 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. e. Lokasi kritikal yang menyimpan maklumat terperingkat hendaklah diasingkan daripada lokasi yang menyimpan maklumat tidak terperingkat.	
4.0	**Kawalan Akses Pusat Data/ Bilik Server**	
	a. Kawalan akses ke pusat data/ bilik server hendaklah ditentukan keselamatannya. Kawalan akses boleh diadakan dalam bentuk seperti berikut: i. Biometrik ii. Katalaluan iii. Sistem elektronik kad pintar dan mekanikal b. Semua akses yang dibenarkan ke kawasan persekitaran pusat data/ bilik server hendaklah diiringi oleh Pentadbir Sistem atau kakitangan teknikal yang dilantik bagi menentukan dan mengawal selia penugasan yang diperlukan. c. Menyediakan buku log untuk tujuan merekodkan maklumat dan aktiviti yang dilaksanakan oleh Pentadbir Sistem ICT atau Pihak Ketiga. d. Sebarang pemindahan maklumat daripada pusat data/ bilik server hendaklah dipohon dan mendapat kebenaran daripada pemilik data (*data owner*) dan Ketua Jabatan masing-masing.	Semua dan Pihak Ketiga
5.0	**Kawalan Persekitaran**	
	a. Bangunan yang menempatkan pusat data/ bilik server hendaklah mempunyai kawalan persekitaran seperti berikut: i. Susunatur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi. ii. Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelak	Semua

	kerosakan komponen elektronik pada perkakasan komputer berkenaan. Pemeriksaan hendaklah dilaksanakan setiap 6 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. b. Bangunan yang menempatkan pusat data/ bilik server hendaklah menentukan ciri-ciri keselamatan seperti berikut: i. Bekalan kuasa elektrik mesti dari punca yang 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 3 bulan bagi menentukan bekalan kuasa berterusan. iii. Sistem pengaliran air yang sempurna bagi mengelakkan banjir. Pemeriksaan terhadap bangunan yang berkenaan hendaklah dilaksanakan setiap 6 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 bekalan kuasa 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	Semua

	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. e. Perangkap kilat *(lightning arrestor)* hendaklah disediakan di semua bangunan penempatan pusat data/ Bilik server bagi mengelakkan kemasukan kuasa elektrik berlebihan *(power surge)* yang disebabkan oleh pancaran kilat.	

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; dan 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, 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-sistem ICT. b. Perisian-perisian yang berfungsi sebagai audio/ video *streaming* dan *peer to peer* adalah dilarang sama sekali. c. Setiap komputer dipasang dengan perisian antivirus yang terkini dan patern virus dikemaskini.	Semua

	d. Untuk mengelak penyebaran atau jangkitan daripada perisian *malicious* semua perisian atau sistem mestilah diimbas dengan antivirus dan diperiksa dan disahkan selamat sebelum digunakan. Ini 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	***Housekeeping***	
	a. Salinan penduaan hendaklah dilakukan seperti berikut : i. Salinan direkodkan dan di simpan di off-site. Lokasi off-site tidak boleh dibangunan yang sama dan pemilihan lokasi mestilah praktikal dengan mengambilkira aspek geografi, kemudahan, keselamatan, kos dan persekitaran. ii. Salinan dilakukan setiap kali konfigurasi berubah. 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; dan v. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu	Semua PTMKN

	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 tindaan	
5.0	**Pengurusan Infrastruktur Rangkaian**	
	a. Pengurusan rangkaian di Jabatan-jabatan Negeri adalah di bawah penyelarasan PTMKN. Segala penyambungan ke atas rangkaian komputer mestilah mendapat kebenaran rasmi PTMKN. b. Pengurusan rangkaian 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 dibenarkan disambungkan kepada Rangkaian Awam tanpa menggunakan mekanisma keselamatan yang diluluskan oleh Jawatankuasa CERT Negeri. e. Semua Jabatan/ Agensi Negeri hendaklah mewujudkan mekanisma 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 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	PTMKN

	diklasifikasikan, didokumenkan dan sentiasa dikemaskini oleh Pentadbir Rangkaian dari semasa ke semasa. j. Semua capaian jarak jauh (*remote access*) tidak dibenarkan melainkan dengan menggunakan sistem autentikasi dan ciri-ciri keselamatan yang dibenarkan oleh Jawatankuasa CERT Negeri. k. Capaian ke Sistem Intranet 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.	
6.0	**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 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 ditempat yang selamat; dan vi. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
7.0	**Keselamatan Komunikasi**	
7.1	**Perkhidmatan Mel Elektronik (e-Mel)**	
	a. Bahagian ini merujuk dan menggunapakai arahan yang tekandung di dalam Pekeliling Kemajuan Pentadbiran Awam Bil.	Semua dan Pentadbir

	1 Tahun 2003. a. Pentadbir Sistem mesti memastikan setiap pelayan e-mel dipasang dengan pelayan antivirus e-mel bagi membolehkan pengimbasan dilakukan sebelum e-mel sampai kepada pengguna. b. Penggunaan kemudahan ini adalah untuk tujuan perkhidmatan rasmi sahaja. c. Semua pihak bertanggungjawab sepenuhnya terhadap semua kandungan e-Mel di dalam akaun sendiri. d. 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. e. Penghantaran maklumat terperingkat melalui Internet mestilah menggunakan kaedah penyulitan yang dibenarkan. f. Sebarang penggunaan e-mel yang boleh memudaratkan nama baik Jabatan / Agensi serta Kerajaan Negeri Pulau Pinang adalah dilarang sama sekali. g. Komunikasi e-mel bagi tujuan rasmi mestilah menggunakan akaun e-mel rasmi kerajaan sahaja. h. Kenyataan Penafian (*Disclaimer)* perlu diletakkan di dalam setiap e-mel rasmi kerajaan seperti : "DISCLAIMER: This e-mel and any files transmitted with it are intended only for the use of the recipient(s) named above and may contain confidential information. You are hereby notified that the taking of any action in reliance upon, or any review, retransmission, dissemination, distribution, printing or copying of this message or any part thereof by anyone other than the recipient(s) is strictly prohibited. If you have received this message in error, you should delete it immediately and advise the sender by return e-mel. Opinions, conclusions and other information in this message that do not relate to the Penang State Government shall be understood as neither given nor endorsed by the Penang State Government." i. 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. j. Elakkan dari membuka e-mel daripada penghantar yang tidak	Sistem ICT

	diketahui dan diragui. k. Mengimbas bahan-bahan yang hendak dimuat naik atau dimuat turun supaya bebas virus sebelum digunakan. l. Semua pihak dilarang daripada melakukan aktiviti 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 disisi 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-udang 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; dan viii. Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.	
7.2	**Perkhidmatan Melayari Internet**	
	a. Bahagian ini merujuk dan menggunapakai arahan yang tekandung 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. 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 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 *social community* atas talian seperti *newsgroup* dan	

	buletin board; 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; 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.	
7.3	**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 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 komersil 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 transaski 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."*	
8.0	**Lain-lain Perkhidmatan**	
	Lain-lain perkhidmatan atau utiliti yang mempunyai risiko terhadap pendedahan maklumat rasmi Jabatan/ Agensi Negeri serta Kerajaan Negeri Pulau Pinang 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 bertangggungjawab terhadapnya. b. Penggunaan teknologi tambahan seperti kad-kad pintar dan teknologi *biometric authentication* perlu dipertimbangkan untuk sistem yang terperingkat. c. Pengguna disarankan menggunakan 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 hakmilik mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan. h. Akaun pengguna akan ditamatkan atas sebab-sebab seperti berikut : i. Bersara; ii. Ditamatkan perkhidmatan; iii. Bertukar ke agensi lain; iv. Bertukar bidang tugas kerja; atau v. Menyalahguna kemudahan akaun ICT yang diberikan. i. Akaun pengguna disaran dibekukan sepanjang tempoh pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh melebihi sebulan.	Semua

2.0	**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
3.0	**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 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 mempastikan kesahihan masa yang tercatat dalam audit log. Pentadbir Sistem harus menentukan penyatuan masa sekurang-kurangnya sekali dalam sebulan.	Pemilik sistem dan Pentadbir Sistem ICT
4.0	**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	Pentadbir Sistem ICT, ICTSO

	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 penyalah gunaan. 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.	
5.0	**Peralatan 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 dan 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/ pemindahan sebarang maklumat jabatan daripada pegawai yang menggunakan komputer riba persendirian sekiranya pegawai tersebut berpindah, bersara atau diberhentikan perkhidmatannya.	Semua
6.0	**Aset ICT**	

	Semua aset ICT mesti dijaga dengan rapi bagi menjamin keselamatannya dari kecurian/ kerosakan dan perlu mendapat kebenaran bertulis 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.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
3.0	**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. Pengunaan tanda tangan 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

4.0	**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 pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
5.0	**Pembangunan dan Proses Sokongan**	
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai.	Pentadbir Sistem ICT

Perkara 10 Perancangan 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 disetuju terima oleh BCSC berkaitan serta diluluskan oleh Jawatankuasa Pemandu eGG. d. Pelan BCP perlu diuji setiap 6 bulan dan disemak sekurang-kurangnya setahun sekali.	Ketua Jabatan dan ICTSO

Perkara 11 Pematuhan

1.0	**Objektif**	Tanggungjawab
	Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT.	
2.0	**Pematuhan Dasar**	
	a. Setiap pengguna Jabatan/ Agensi Negeri hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuatkuasa. b. Semua aset ICT termasuk maklumat yang disimpan di dalamnya adalah hakmilik Kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
3.0	**Keperluan Perundangan dan Peraturan**	
	Berikut adalah keperluan perundangan dan peraturan-peraturan lain 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	Semua

	h. Akta Jenayah Komputer 1997 i. Akta Hak cipta (Pindaan) Tahun 1997 j. Akta Komunikasi dan Multimedia 1998.	

RUJUKAN

[1] "Dasar Keselamatan ICT," MAMPU, Ed.: Jabatan Perdana Menteri, 2006.

[2] "Malaysian Public Sector ICT Security Risk Assessment Methodology," in *Surat Pekeliling Am*. vol. Bil 6: Jabatan Perdana Menteri, 2005.

[3] "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan," in *Pekeliling Am*. vol. Bil 1: Jabatan Perdana Menteri, 2003.

[4] "Dasar Keselamatan ICT ", B. T. Maklumat, Ed.: Kementerian Pertahanan Malaysia, 2002.

[5] "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)," in *Pekeliling Am*. vol. Bil. 1: Jabatan Perdana Menteri, 2001.

[6] "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan," in *Pekeliling Am*. vol. Bil 3: Jabatan Perdana Menteri, 2000.

[7] *Arahan Keselamatan Malaysia*. Malaysia.

[8] BTMK, *Dasar Keselamatan ICT KKM*: Kementerian Kesihatan Malaysia, 2007.

[9] MAMPU, *Arahan Teknologi Maklumat*: Jabatan Perdana Menteri, 2007.

[10] MAMPU, "Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam," J. P. Menteri, Ed.: MAMPU, 2006, p. 29.

[11] MAMPU, "Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)," MAMPU, 2002.

[12] MAMPU, "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" in *Pekeliling Kemajuan dan Pentadbiran Am.* vol. 1: Jabatan Perdana Menteri, 2003.

[13] SIRIM, *MS ISO/IEC 27001 Information Security Management System Standard*. Malaysia, 2006.

LAMPIRAN A

STRUKTUR ORGANISASI KESELAMATAN ICT NEGERI