DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

NEGERI PULAU PINANG

9 JUN 2010

VERSI 1.0

Dasar Keselamatan ICT Negeri versi 1.0 ini telah dibentangkan dan diluluskan oleh Jawatankuasa *Electronic Good Governance* (eGG) pada 9 Jun 2010.

Dasar Keselamatan ICT versi 1.0 ini dipanjangkan kepada semua Jabatan Negeri untuk diterima pakai manakala Agensi Negeri dan Pihak Berkuasa Tempatan Negeri adalah tertakluk kepada penerimaan oleh pihak berkuasa masing-masing.

DATO' ZAINAL RAHIM BIN SEMAN
Setiausaha Kerajaan Negeri
Pulau Pinang

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
15 Januari 2009	0.0	Mesyuarat JKP eGG Bil. 1/2009	27 Februari 2009
9 Jun 2010	1.0	Mesyuarat JKP eGG Bil. 2/2010	22 Julai 2010

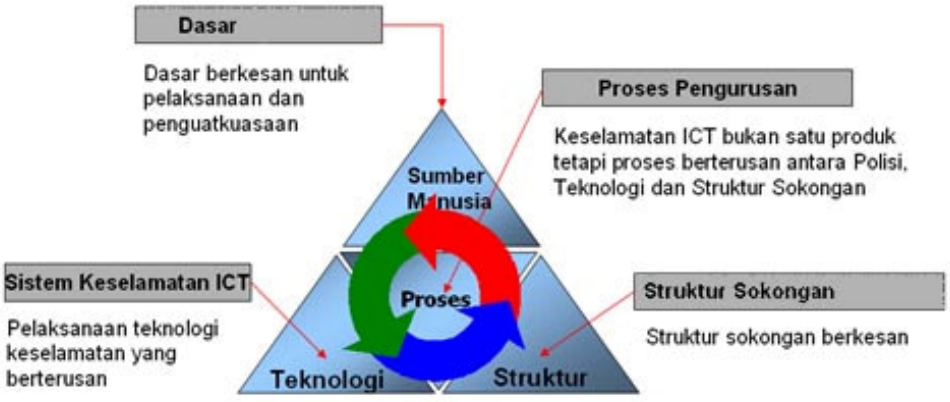
Kandungan

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.

PENILAIAN RISIKO KESELAMATAN ICT

Jabatan/Agensi Negeri hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu, Jabatan/Agensi Negeri perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Jabatan/Agensi Negeri 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 Jabatan/Agensi Negeri 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 utiliti dan sistem-sistem sokongan lain.

Jabatan/Agensi Negeri bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bil 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Jabatan/Agensi Negeri perlu mengenalpasti tindkan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut :

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

BIDANG 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
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 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 atau mengikut keperluan semasa.	ICTSO
4.0	**Pengecualian Dasar**	
	Dasar Keselamatan ICT Negeri adalah terpakai kepada semua pengguna ICT Jabatan/Agensi Negeri dan tiada pengecualian diberikan.	Semua

BIDANG 02 ORGANISASI KESELAMATAN

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 1**.	
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 pematuhan 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

5.0	**Pengurus ICT**	
	Peranan dan tanggungjawab adalah termasuk seperti berikut : a. Mengkaji semula dan melaksanakan kawalan keselamatan selaras dengan keperluan ICT Kerajaan; b. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; c. Menentukan kawalan akses semua pengguna terhadap aset ICT Kerajaan; d. Menentukan tahap kawalan akses semua pengguna terhadap aset ICT Kerajaan; e. Melaporkan sebarang perkara atau penemuan mengenai ancaman keselamatan ICT kepada ICTSO; dan f. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT.	Pengurus 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;	Semua

	b. Mengetahui dan memahami implikasi keselamatan ICT kesan dan tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat; d. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; e. Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan katalaluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT seperti di **Lampiran 2**.	
8.0	**Pihak Ketiga**	
	Perkara yang perlu dipatuhi termasuk yang berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang	Semua

	sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Akses kepada aset ICT Jabatan/Agensi Negeri perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Kandungan perjanjian kontrak dengan pihak ketiga perlu merangkumi perkara-perkara berikut : i. Dasar Keselamatan ICT ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972 Bagi Penjawat Bukan Awam; dan iv. Hak Harta Intelek g. Pihak ketiga perlu menandatangani dokumen-dokumen berikut bagi melindungi aset ICT Kerajaan : a. Surat akuan pematuhan Dasar Keselamatan ICT seperti di **Lampiran 2**; dan b. Perakuan Akta Rahsia Rasmi 1972 Bagi Bukan Penjawat Awam seperti di **Lampiran 3.**	
9.0	**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 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.	J/kuasa Pemandu eGG

	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.	
10.0	**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 Pusat Teknologi Maklumat dan Komunikasi Negeri (PTMKN) – Pengerusi b. Pegawai Teknologi Maklumat (Kanan), Unit Keselamatan dan Pangkalan Data PTMKN c. Pegawai Teknologi Maklumat (Kanan), Unit Rangkaian, Operasi dan Sokongan Teknikal PTMKN d. Pegawai Teknologi Maklumat (Kanan), Unit Pembangunan Sistem dan Portal PTMKN e. Wakil Jabatan Kewangan Negeri f. Wakil Pejabat Tanah dan Galian Negeri g. Wakil Jabatan Agama Islam Pulau Pinang h. Wakil PEGIS i. Wakil Pejabat Daerah dan Tanah seluruh Pulau Pinang j. Wakil Perpustakaan Negeri Pulau Pinang k. Urusetia -PTMKN Tugas dan tanggungjawab Jawatankuasa ini adalah seperti berikut: a. Menilai aspek-aspek teknikal berhubung inisiatif dan projek keselamatan ICT. b. Memberi nasihat teknikal kepada Jawatankuasa Pemandu *eGG*. c. Menyediakan pelan tindakan untuk pembangunan dan peningkatan keselamatan sistem ICT.	J/kuasa CERT Negeri

	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*.	
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 J/kuasa CERT Agensi

BIDANG 03 PENGURUSAN ASET

1.0	**Objektif**	Tanggungjawab
	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.	
2.0	**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. b. Semua aset ICT mesti dijaga dengan rapi bagi menjamin keselamatannya dari kecuiran/kerosakan dan perlu mendapat kebenaran bertulis Ketua Jabatan untuk dibawa keluar sekiranya ada maklumat terperingkat. c. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem ICT Semua
3.0	**Pengelasan 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
4.0	**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;	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 pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

BIDANG 04 KESELAMATAN SUMBER MANUSIA

1.0	**Objektif**	Tanggungjawab
	Memastikan kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan ICT. Ini bertujuan bagi meminimumkan risiko kesilapan manusia, kecuaian, penipuan, kecurian maklumat, pemalsuan identiti dan penyalahgunaan kemudahan.	
2.0	**Sebelum Perkhidmatan**	
	Perkara yang perlu dipatuhi adalah seperti berikut : a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan mestilah dinyatakan dengan lengkap dan jelas; b. Menjalankan tapisan keselamatan untuk calon kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan hendaklah berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarka perjanjian yang telah ditetapkan.	Semua
3.0	**Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a. Memastikan kakitangan Jabatan/Agensi Negeri dan pihak ketiga yang berkepentingan menguruskan keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Jabatan/Agensi Negeri; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua kakitangan	Semua

	Jabatan/Agensi Negeri dan sekiranya perlu kepada pihak ketiga dari semasa ke semasa; dan c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas kakitangan Jabatan/Agensi Negeri dan pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh Jabatan/Agensi Negeri; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
4.0	**Tamat Perkhidmatan atau Bertukar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan semua aset ICT Jabatan/Agensi Negeri dikembalikan kepada Jabatan/Agensi Negeri mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan/Agensi Negeri dan/atau terma perkhidmatan.	Semua
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	Semua

	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/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.	

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

1.0	**Objektif**	**Tanggungjawab**
	Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
2.0	**Keselamatan Kawasan**	
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara berikut yang perlu dipatuhi termasuk berikut : a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memasang alat penggera atau kamera; d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh masuk melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan	Pejabat Ketua Pegawai Keselamatan/ Pegawai Keselamatan Pejabat, CIO dan ICTSO

	l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
2.1	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi termasuk berikut : a. Setiap kakitangan Jabatan/Agensi Negeri hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada Jabatan/Agensi Negeri apabila kakitangan berhenti atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter pengawal Jabatan/Agensi Negeri; dan d. Kehilangan pas mestilah dilaporkan dengan segera.	Pentadbir Sistem ICT dan Pihak Ketiga
2.2	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. a. Kawasan larangan adalah Pusat Data/ Bilik Server dan Pusat *Disaster Recovery Center* (DRC). b. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan c. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua dan Pihak Ketiga
2.3	**Kawalan 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	Semua dan Pihak Ketiga

	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. e. Mempunyai alat penghawa dingin yang mempunyai keupayaan mengawal kelembapan udara bagi mengelak kerosakan komponen elektronik pada perkakasan komputer berkenaan. f. Menyediakan sistem pengudaraan *(ventilation)* yang mencukupi. g. Penggunaan lantai bertingkat *(raised floor)* dalam pusat data/ bilik server. h. Penggunaan kamera boleh dilaksanakan bagi meningkatkan kawalan keselamatan. i. 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. j. Perangkap kilat *(lightning arrestor)* hendaklah disediakan di bangunan penempatan pusat data/ Bilik server bagi mengelakkan kemasukan kuasa elektrik berlebihan *(power surge)* yang disebabkan oleh pancaran kilat.	
3.0	**Keselamatan Peralatan ICT**	
	Ini bertujuan untuk melindungi peralatan ICT Jabatan/Agensi Negeri dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :	Semua

	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 dikemaskini 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 kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti switches, hub, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; k. Peralatan ICT yang hendak dibawa keluar dari premis Jabatan/Agensi Negeri perlulah mendapat kelulusan Pentadir Sistem ICT dan direkodkan bagi tujuan pemantauan; l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;	

	m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; p. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; r. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t. Pengguna hendaklah memastikan semua perkakassan komputer, pencetak dan pengimbas dalam keadaan 'OFF' apabila meninggalkan pejabat; u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan v. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
3.1	**Media Storan**	
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan	Semua

	untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup)* pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
3.2	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Jabatan/Agensi Negeri; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, disk atau media	Semua

	berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
3.3	**Perkhidmatan dan Penyelenggaraan**	
	a. 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; b. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; 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; dan 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
3.4	**Peralatan di Luar Premis**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
3.5	**Pelupusan Perkakasan**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Kerajaan Negeri dan ditempatkan di Jabatan/Agensi	Pegawai Aset, PTMKN dan Bahagian ICT

	Negeri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya tidak terlepas dari kawalan Jabatan/Agensi Negeri. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum pindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenalpasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi mejamin keselamatan peralatan tersebut; f. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori semasa. g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa; dan h. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara berikut : i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *harddisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran	Jabatan/Agensi Negeri

	komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan/Agensi Negeri; iii. Memindah keluar dari Jabatan/Agensi Negeri mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT; i. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
4.0	**Kawalan Persekitaran**	
	Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan ditempat yang bersesuaian dan berjauhan dari aset ICT; f. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;	Semua
4.1	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.	PMTKN, Bahagian ICT

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Bekalan kuasa elektrik mesti dari punca yang berasingan dan berkemampuan menampung semua beban termasuk server, alat penghawa dingin, alat penggera dan lain-lain. c. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana bekalan kuasa (*Generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan dan diuji setiap 3 bulan bagi menentukan bekalan kuasa berterusan; dan d. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Jabatan/Agensi Negeri dan ICTSO
4.2	**Kabel**	
	Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	PTMKN, Bahagian ICT Jabatan/Agensi Negeri dan ICTSO
5.0	**Keselamatan Dokumen**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : 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	Semua

	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; dan e. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI

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	**Pengendalian Prosedur Operasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklak didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
3.0	**Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Semua

	c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
4.0	**Pengasingan Tugas dan Tanggungjawab**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT dan ICTSO
5.0	**Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**	
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut : a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan di audit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
6.0	**Perancangan Dan Penerimaan Sistem**	
	a. Kapasiti sesuatu komponen atau sistem ICT hendaklah	Pentadbir

	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.	Sistem ICT, ICTSO
7.0	**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. Sekiranya teknologi ini perlu digunakan bagi tujuan rasmi, permohonan kebenaran khas perlulah dikemukakan kepada PTMKN untuk pertimbangan dan kelulusan YB Setiausaha Kerajaan. Bagi Agensi Negeri, permohonan hendaklah dikemukakan kepada Bahagian ICT Agensi untuk kelulusan Ketua Agensi masing-masing. c. Setiap komputer dipasang dengan perisian antivirus yang terkini dan patern virus 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. Ini merangkumi juga setiap media storan luar yang dibawa masuk.	Semua

	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. j. Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
8.0	***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. Kekerapan salinan dilakukan bergantung pada tahap kritikal maklumat; 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. Menyimpan sekurang-kurangnya tiga (3) generasi salinan penduaan; dan vi. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai	Semua PTMKN dan Bahagian ICT Jabatan/Agensi Negeri

	dan berkesan apabila digunakan khususnya pada waktu kecemasan.	
9.0	**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 diklasifikasikan, didokumenkan dan sentiasa dikemaskini oleh Pentadbir Rangkaian dari semasa ke semasa. j. Semua capaian jarak jauh (*remote access*) tidak dibenarkan	PTMKN dan Bahagian ICT Jabatan/Agensi Negeri

	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. m. Semua pengguna hanya dibenarkan menggunakan rangkaian sahaja dan pengunaan modem atau *wireless* broadband pada peralatan pejabat adalah dilarang sama sekali. n. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
10.0	**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
11.0	**Keselamatan Sistem Dokumentasi**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan	Semua

	sistem dokumentasi adalah seperti berikut : a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	
12.0	**Keselamatan Komunikasi**	
12.1	**Pengurusan Pertukaran Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Jabatan/Agensi Negeri dengan Agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Jabatan/Agensi Negeri; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
12.2	**Pengurusan Mel Elektronik (e-Mel)**	
	a. Bahagian ini merujuk dan menggunapakai arahan yang terkandung di dalam Surat Pekeliling Setiausaha Kerajaan Bil 3 Tahun 2010 : Polisi E-mel Rasmi Kerajaan Negeri Pulau Pinang/ 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	Semua dan Pentadbir Sistem ICT

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 yang dibenarkan.

g. Sebarang penggunaan e-mel yang boleh memudaratkan nama baik Jabatan/Agensi serta Kerajaan Negeri Pulau Pinang 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 :

> "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."

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. Semua pihak dilarang daripada melakukan aktiviti yang melanggar tatacara penggunaan e-mel rasmi kerajaan seperti yang telah digariskan di dalam Polisi Emel Rasmi Kerajaan Negeri Pulau Pinang.

n. Sebarang pelanggaraan polisi penggunaan emel akan

	dilaksanakan seperti yang telah digariskan di dalam Polisi Emel Rasmi Kerajaan Negeri Pulau Pinang atau mengikut polisi Agensi berkenaan.	
12.3	**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. 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;	Semua

	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, buletin board, facebook, twitter, flickers* dan seumpamanya; 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; i. Komputer peribadi yang digunakan untuk mencapai internet mesti dilengkapi dengan ciri-ciri keselamatan tambahan seperti perisian Antivirus dan Anti-Spyware. j. Penggunaan peralatan/ perisian *Proxy Avoidance* adalah dilarang sama sekali.	
13.0	**Perkhidmatan Laman Web**	
	a. Notis hakcipta perlu diletakkan pada semua laman web rasmi	Semua dan

	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."*	Pentadbir Sistem ICT
13.1	**Perkhidmatan e-Dagang**	
	Memastikan keselamatan perkhidmatan e-Dagang dan penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut : a. Maklumat yang terlibat dalam e-Dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelakkan penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti maklumat yang disediakan dalam sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang	Semua

	tidak diperakukan.	
14.0	**Pemantauan**	
14.1	**Pengauditan dan Forensik ICT**	
	ICTSO mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut : a. Sebarang percubaan pencerobohan kepada sistem ICT Jabatan/Agensi Negeri. b. Serangan kod perosak (*malicious code*), halagan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery*, *phishing*), 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; dan h. Aktiviti penukaran alamat IP *(IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO
14.2	**Jejak Audit**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua perkakasan/ utiliti mestilah mengaktifkan audit log. Audit log perlu disimpan untuk tempoh masa yang dipersetujui 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 ICT mestilah dilogkan.	Pemilik sistem dan Pentadbir Sistem ICT

	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 ICT secara automatik sebagai tanda peringatan. f. Pentadbir Sistem ICT 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.	
14.3	**Sistem Log**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
14.4	**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 memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada	Pentadbir Sistem ICT dan ICTSO

	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; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan/Agensi Negeri atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
15.0	**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.	Semua

BIDANG 07 KAWALAN CAPAIAN

1.0	**Objektif**	**Tanggungjawab**
	Mengawal capaian ke atas maklumat.	
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 (8) aksara bagi pengguna dengan mempunyai kombinasi huruf, nombor dan aksara khas manakala dua belas (12) aksara bagi pentadbir sistem dengan 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	Semua

	pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh melebihi sebulan.	
3.0	***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 di 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; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua
4.0	**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
4.1	**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.	Pentadbir Sistem ICT, ICTSO

	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. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. b. Instalasi perisian komputer mudah alih mestilah dilaksanakan oleh kakitangan ICT. c. Komputer mudah alih hendaklah sentiasa di bawah penjagaan yang rapi bagi menjamin keselamatannya dari kecurian dan kerosakan. d. Pengguna yang membawa maklumat terperingkat dikehendaki mengisytiharkannya dengan mendapat kebenaran bertulis dari Ketua Jabatan atau setaraf. e. 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. f. 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
5.1	**Kerja Jarak Jauh**	
	Perkara yang perlu dipatuhi adalah seperti berikut : a. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak	Semua

	sah serta salah guna kemudahan.	

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

1.0	**Objektif**	**Tanggungjawab**
	Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
2.0	**Keperluan Keselamatan Sistem Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
2.1	**Pengesahan Data Input dan Output**	
	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.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO

3.0	**Kawalan 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. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. d. Data ujian perlu dipili dengan berhati-hati, dilindungi dan dikawal. e. Mengaktifkan audit log bagi merekodkan semua pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
5.0	**Keselamatan dalam Proses Pembangunan dan Sokongan**	
	a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu	Pemilik Sistem dan Pentadbir Sistem ICT

	bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	
5.1	**Pembangunan Perisian Secara *Outsource***	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan *Outsourcing* perlu dikawal daripada segi perlaksanaannya bagi menjamin keselamatan terhadap sistem yang akan dilaksanakan secara *outsource*. b. Kaedah pelaksanaan *outsourcing* adalah berdasarkan kepada Garis Panduan IT *Outsource* Agensi-Agensi Sektor Awam. c. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah hak milik Kerajaan.	Pemilik Sistem dan Pentadbir Sistem ICT
6.0	**Kawalan Teknikal Keterdedahan (*Vulnerability*)**	
	Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-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 mengenalpasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

1.0	**Objektif**	Tanggungjawab
	Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimakan kesan insiden keselamatan ICT.	
2.0	**Prosedur Pengurusan Insiden**	
	Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan audit trail dan memelihara bahan bukti; dan d. Menyediakan pelan tindakan pemulihan segera.	ICTSO
3.0	**Pelaporan Insiden**	
	Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO dengan kadar segera. Insiden keselamatan ICT adalah termasuk yang berikut : 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 disyaki digunakan tanpa kebenaran dan kecurian maklumat/data; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang; d. Berlaku kejadian sistem luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi dan kesilapan/ralat dalam komunikasi data; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.	Semua

	Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di Negeri Pulau Pinang adalah seperti di **Lampiran 4.**	
4.0	**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 datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Kerajaan Negeri Pulau Pinang. Bahan-bahan bukti berkaitan insiden keselamatan ICT 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; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

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. Perkara-perkara berikut perlu diberi perhatian : i. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; ii. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut akibat terhadap keselamatan ICT; iii. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat	Ketua Jabatan dan ICTSO

	mungkin atau dalam jangka masa yang telah ditetapkan; iv. Mendokumentasikan proses dan prosedur yang telah dipersetujui; v. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; vi. Membuat *backup*; dan vii. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. d. Pelan BCP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut : i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; ii. Senarai personel Jabatan/Agensi Negeri dan pembekal beserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; iii. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; iv. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan v. Perjanjian dengan pembekal perkhdimatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. e. Salinan pelan BCP perlu disimpan dilokasi berasingan untuk mengelakkan kerosakan akibat bencana dilokasi utama. Pelan BCP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. f. Ujian pelan BCP hendaklah dijadualkan untuk memastikan semua	

	ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	

BIDANG 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. c. Sebarang pengunaan aset ICT Jabatan/Agensi Negeri selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber Jabatan/Agensi Negeri.	Semua
3.0	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	a. ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. b. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
4.0	**Pematuhan Keperluan Audit**	
	a. Naziran boleh dilaksanakan secara mengejut atau secara berjadual bagi memastikan keselamatan ICT; b. Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat; c. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan	Semua

	perkhidmatan; dan d. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
5.0	**Keperluan Perundangan dan Peraturan**	
	Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di Jabatan/Agensi Negeri adalah seperti di **Lampiran 5**.	Semua
6.0	**Perlanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT boleh dikenakan tindakan tatatertib.	Semua

RUJUKAN

[1] "Dasar Keselamatan ICT ver. 5.3," MAMPU, Ed.: Jabatan Perdana Menteri, 2010.

[2] "Polisi Emel Rasmi Kerajaan Negeri Pulau Pinang," Pejabat Setiausaha Kerajaan Negeri Pulau Pinang, Ed.: Pusat Teknologi Maklumat dan Komunikasi Negeri, 2010.

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

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

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

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

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

[8] *Arahan Keselamatan Malaysia*. Malaysia.

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

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

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

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

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

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.
Bahagian ICT Agensi	Bahagian ICT adalah satu bahagian di bawah sesuatu Agensi Negeri yang mempunyai pasukan ICT sendiri.
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.

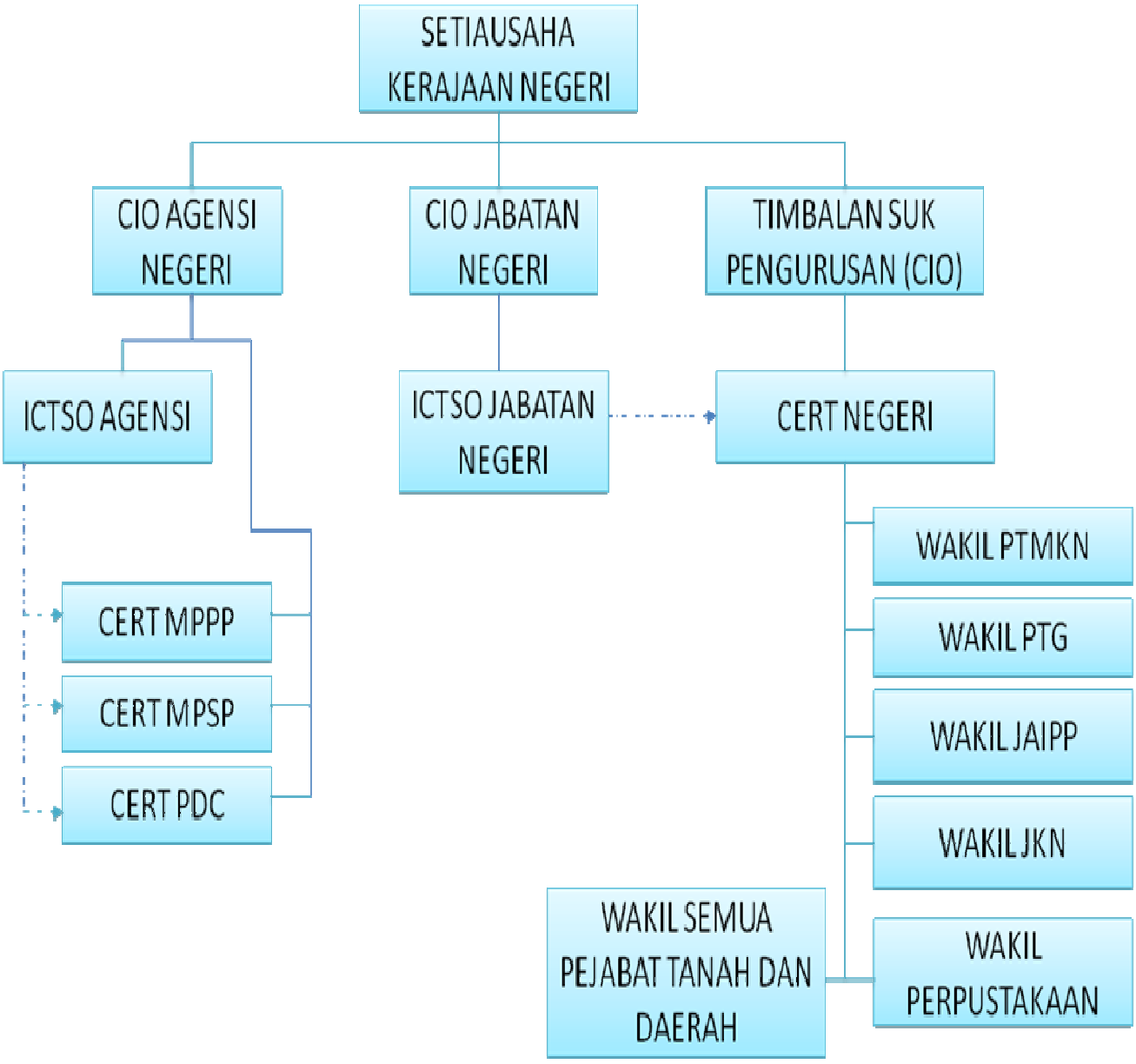
Internet	Perkhidmatan informasi secara global yang menghubungkan semua pengguna seluruh dunia melalui satu protokol rangkaian.
Information Security	Proses dan mekanisme untuk melindungi maklumat.
Jawatankuasa Pemandu *Electronic Good Governance (eGG)*	Jawatankuasa ICT Tertinggi di peringkat Kerajaan 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/ broadband	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.

LAMPIRAN 1

STRUKTUR ORGANISASI KESELAMATAN ICT NEGERI



LAMPIRAN 2

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT NEGERI PULAU PINANG

Saya, ……
No Kad Pengenalan : ……

dengan sesungguhnya berjanji bahawa saya akan mematuhi peruntukan Dasar Keselamatan Teknologi Maklumat dan Komunikasi Negeri Pulau Pinang serta apa-apa peraturan dan arahan lain yang berkaitan yang dikeluarkan dan dikuatkuasakan dari semasa ke semasa sepanjang tempoh perkhidmatan saya. Maka dengan itu saya berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan Teknologi Maklumat dan Komunikasi Negeri Pulau Pinang.

Saya sesungguhnya faham bahawa jika saya disabitkan kerana telah melanggar Dasar Keselamatan Teknologi Maklumat dan Komunikasi Negeri ini, saya boleh dikenakan tindakan tatatertib mengikut Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 atau Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) (Pulau Pinang)1997.

…… ……
(Tandatangan Pegawai) (Jawatan Pegawai)

Di hadapan saya,

……..
(Tandatangan Ketua Jabatan)

…… ……
(Tarikh) (Cop Rasmi Jabatan)

LAMPIRAN 3

PERAKUAN UNTUK DITANDATANGANI OLEH MEREKA YANG BUKAN PENJAWAT AWAM/PAKAR PERUNDING BERKENAAN DENGAN AKTA RAHSIA RASMI 1972 (AKTA 88)

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 (Akta 88) dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia Kerajaan, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa sebagai kakitangan syarikat kontraktor atau subkontraktor dengan Kerajaan Malaysia, segala rahsia rasmi yang saya peroleh dalam perkhidmatan Seri Paduka Baginda Yang dipertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang dipertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kontraktor Kerajaan.

Tandatangan:.....

Nama (Huruf Besar):.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/Organisasi:.....

Tarikh:.....

Disaksikan Oleh:.....
(Tandatangan)

Nama (Huruf Besar):.....

No. Kad Pengenalan:.....

Jawatan : .....

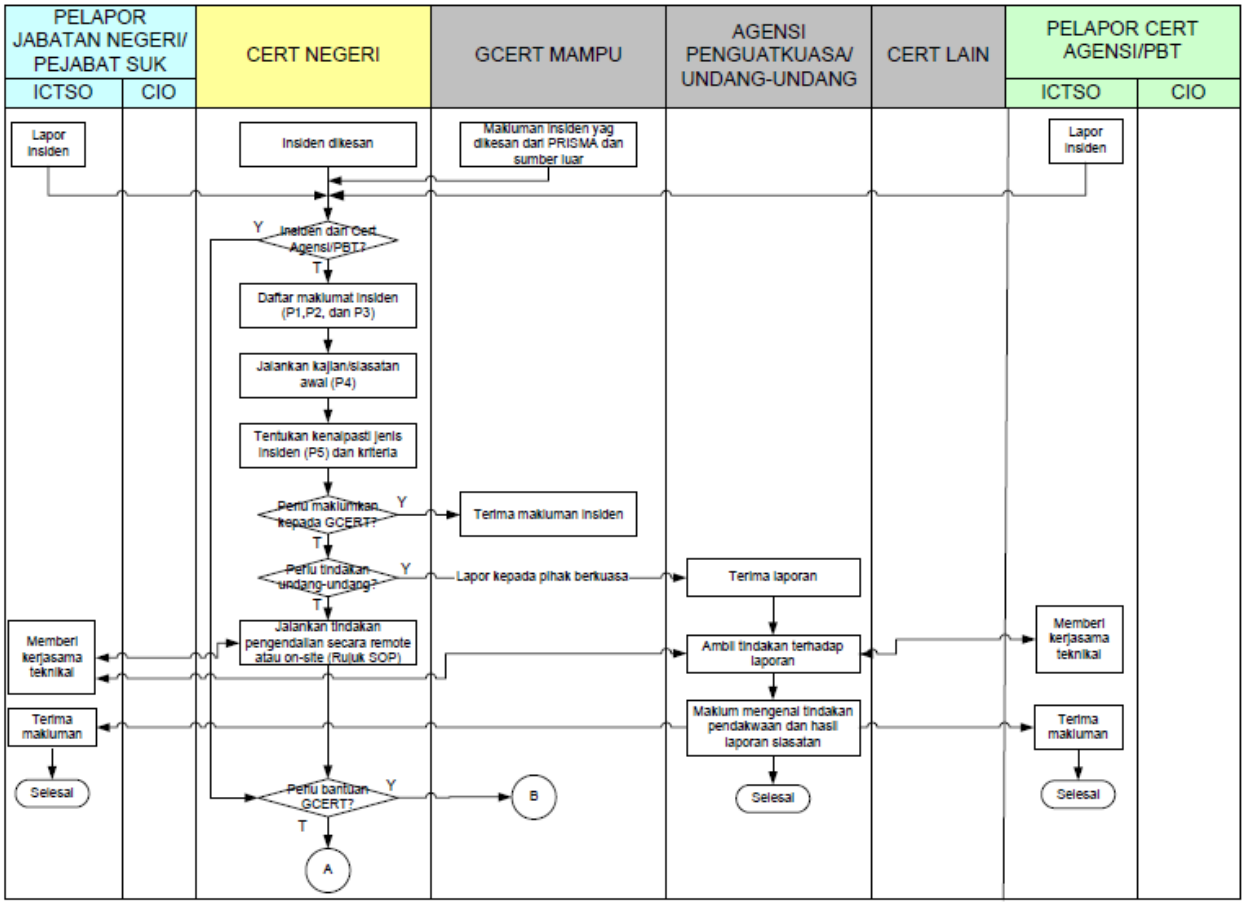
Jabatan/Organisasi:.....

Tarikh:.....

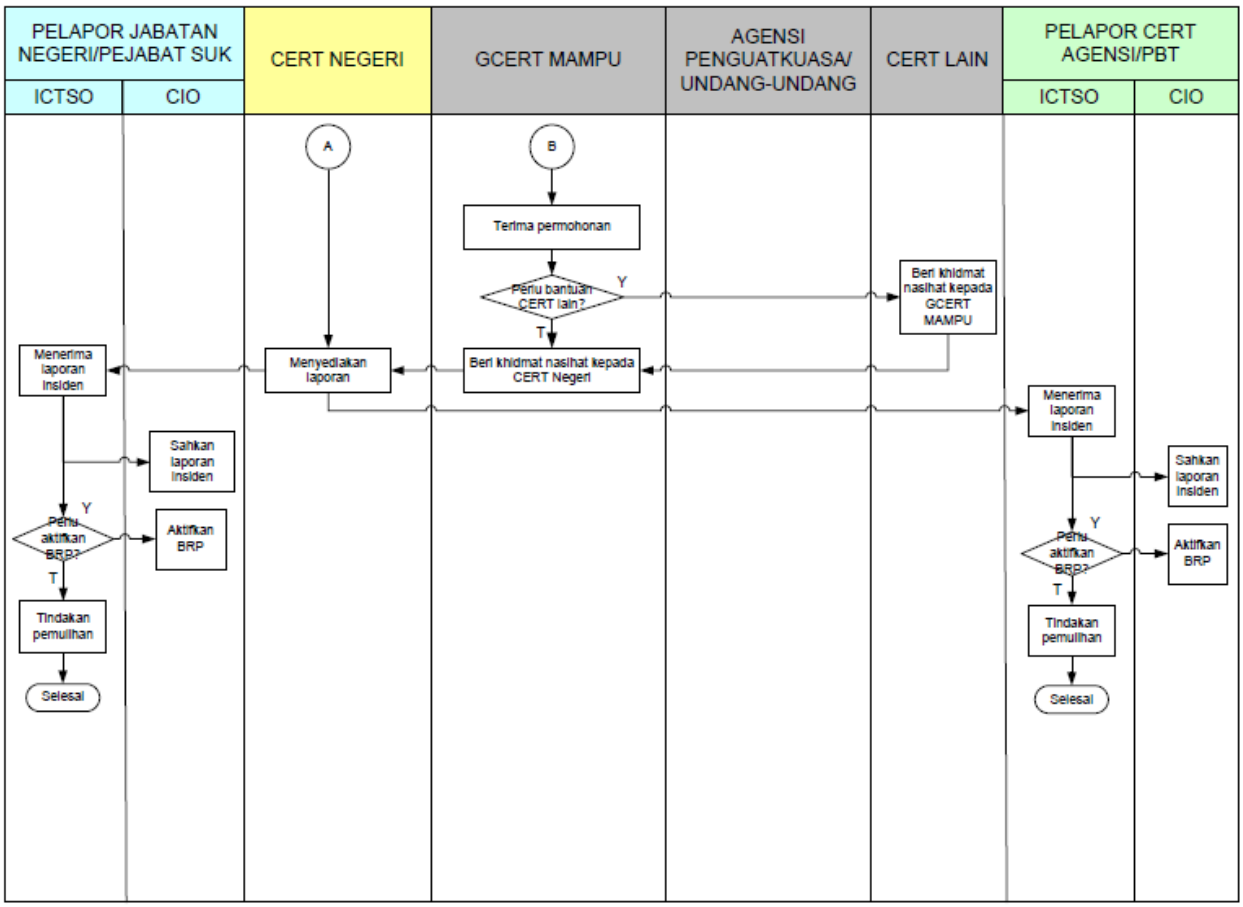
Cop Jabatan/Organisasi:.....

LAMPIRAN 4

RINGKASAN CARTA ALIR PROSES KERJA PENGENDALIAN INSIDEN KESELMATAN ICT CERT NEGERI



RINGKASAN CARTA ALIR PROSES KERJA PENGENDALIAN INSIDEN KESELMATAN ICT CERT NEGERI



LAMPIRAN 5

SENARAI PERUNDANGAN DAN PERATURAN

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. Surat Pekeliling Setiausaha Kerajaan Bil 3 Tahun 2010 : Polisi E-mel Rasmi Kerajaan Negeri Pulau Pinang.

h. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

i. Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

j. Surat Arahan Ketua Penggarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

k. Akta Tandatangan Digital 1997;

l. Akta Jenayah Komputer 1997;

m. Akta Hak cipta (Pindaan) Tahun 1997;

n. Akta Komunikasi dan Multimedia 1998;

o. Perintah-Perintah Am;

p. Arahan Perbendaharaan; dan

q. Arahan Teknologi Maklumat 2007;