DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

NEGERI PULAU PINANG

17 NOVEMBER 2016

VERSI 2.0

Dasar Keselamatan ICT Negeri versi 2.0 ini telah dibentangkan dan diluluskan oleh Jawatankuasa *Electronic Good Governance* (eGG) pada 25 Februari 2016.

Dasar Keselamatan ICT versi 2.0 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' SERI FARIZAN BIN DARUS
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
21 September 2011	1.1	Mesyuarat JKP eGG Bil. 3/2011	18 Oktober 2011
14 Disember 2012	1.2	Mesyuarat JKP eGG Bil. 4/2012	24 Disember 2012
17 Disember 2013	1.3	Mesyuarat JKP eGG Bil. 4/2013	27 Disember 2013
25 Februari 2016	2.0	Mesyuarat JKP eGG Bil. 1/2016	17 November 2016

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
25 Februari 2016	2.0	i. Pindaan adalah bagi memenuhi keperluan ISO/IEC 27001:2013 – ISMS ii. Kajian Semula DKICT dipinda daripada sekurang-kurangnya sekali dalam tempoh setahun kepada sekurang-kurangnya dua tahun sekali iii. Garis Panduan BYOD dimasukkan dalam Kawalan Polisi Peranti Mudah Alih iv. Penambahan 11 Kawalan Baru • **2.1.5** Keselamatan Maklumat Dalam Pengurusan Projek. • **8.6.2** Kawalan Pemasangan Perisian. • **10.2.1** Dasar Keselamatan Dalam Pembangunan Sistem. • **10.2.5** Prinsip Kejuruteraan Keselamatan Sistem. • **10.2.6** Keselamatan Persekitaran Pembangunan Sistem. • **10.2.8** Pengujian Keselamatan Sistem. • **11.1.1** Dasar Keselematan Maklumat Untuk Pembekal. • **11.1.3** Kawalan Rantaian Bekalan Maklumat dan Komunikasi. • **12.1.4** Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat.

TARIKH	VERSI	BUTIRAN PINDAAN
		• **12.1.5** Pengurusan Maklumat Insiden Keselamatan ICT. • **13.2.1** Ketersediaan Kemudahan Pemprosesan Maklumat.
17 Disember 2013	1.3	i. Bidang 01: Para 10.0 muka surat 14, pindaan kepada senarai keahlian Jawatankuasa CERT Negeri ditambah : k. Wakil Jabatan Perancang Bandar dan Desa l. Wakil Jabatan Kehakiman dan Syariah Negeri m. Wakil Jabatan Kebajikan Masyarakat ii. Bidang 04: para 4.0 muka surat 19, pindaan tambahan klausa : c. Pegawai/ kakitangan menandatangani perakuan berkenaan Akta Rahsia Rasmi 1972 apabila meninggalkan Perkhidmatan Kerajaan. iii. Senarai Perundangan Dan Peraturan, tambahan bahan rujukan “Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan”, Pejabat Setiausaha Kerajaan Negeri Pulau Pinang, 2013.
14 Disember 2012	1.2	i. PRINSIP DASAR KESELAMATAN ICT f.Pematuhan para 3 muka surat 5,pindaan PTMKN/Unit ICT Agensi Negeri kepada

TARIKH	VERSI	BUTIRAN PINDAAN
		PTMKN/Bahagian ICT Jabatan / Agensi Negeri ii. Bidang 01:Para 4.0 muka surat 8, pindaan kepada Dasar Keselamatan ICT Negeri adalah terpakai kepada semua pengguna ICTJabatan Negeri tanpa pengecualian. Manakala bagi Agensi Negeri tertakluk kepada penerimaan agensi iii. Bidang 02:Para 7.0 (h) muka surat 12 Menandatangani surat akuan pematuhan Dasar Keselamatan ICTsekali setiap tahun. iv. Bidang 02:Para 8(e) muka surat 13 pindaan kepada i. Terma-terma bersesuaian di dalam DKICT ii. Perakuan Akta Rahsia Rasmi 1972 Bagi Penjawat Bukan Awam; dan iii. Hak Harta Intelek v. Bidang 04:Para 3.0 muka surat 19 penambahan klausa (e) Menandatangani surat akuan

TARIKH	VERSI	BUTIRAN PINDAAN
		pematuhan Dasar Keselamatan ICT bagi kakitangan baru(pengambilan baru/perpindahan). vi. Bidang 04:Para 5(a) muka surat 20 pindaan nombor tol free kepada nombor bebas tol. vii. Bidang 04:Para 5 (d) muka surat 20 pindaan kepada Menerima sebarang permohonan atau pertanyaan untuk mendapatkan sebarang maklumat berkaitan jabatan perlulah disertakan surat rasmi. Penyaluran maklumat perlulah mendapat kelulusan Ketua Jabatan. viii. Bidang 05:Para 2.3 muka surat 23 (k) Memasang UPS dan/atau GENSET sebagai perlindungan kepada aset ICT sewaktu gangguan bekalan elektrik. (l) Memasang Heat Sensor dan Smoke detector adalah disyorkan sebagai alat pengesahan perubahan persekitaran. (m) Disyorkan memasang talian telefon untuk memudahkan perhubungan. ix. Bidang 05:Para 3.0 (v) muka surat 25, Menutup suis dan menanggalkan palam kuasa bagi mengelakkan kerosakan perkakasan sebelum

TARIKH	VERSI	BUTIRAN PINDAAN
		meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. x. Bidang 6.0: Para 9.0 (g) muka surat 36 pindaan Sebarang pengujian perkakasan, perisian dan sistem aplikasi hendaklah mendapat kebenaran daripada Pentadbir Sistem. Perkakasan / sistem aplikasi yang baru dibangunkan/peningkatan perlu disemak tahap keselamatan dengan menggunakan peralatan imbasan yang bersesuaian oleh PTMKN / Bahagian ICT Agensi Negeri sebelum boleh diaktifkan bagi menjamin keselamatan aset ICT kerajaan xi. Bidang 6.0: Para 9.0 (m) muka surat 37 Semua pengguna hanya dibenarkan menggunakan kemudahan rangkaian yang disediakan dan pengunaan modem / wireless serta broadband persendirian pada peralatan pejabat adalah dilarang sama sekali. xii. Bidang 6.0: Para 9.0 (n) muka surat 37 Penyediaan kemudahan wireless LAN di pejabat perlu mendapat kelulusan JPPICT dan dipastikan kawalan keselamatan.

TARIKH	VERSI	BUTIRAN PINDAAN
		xiii. Bidang 7.0: Para 5.0 muka surat 48, pindaan tajuk Peralatan Komputer Mudah Alih/Riba kepada Peralatan Komputer Mudah Alih. Pindaan para 5.0 (a) muka surat 48 pindaan Peralatan komputer mudah alih (seperti laptop dan tablet) hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. xiv. Bidang 7.0:Para 5.0 (e) muka surat 48, pindaan kepada Pengguna yang menggunakan komputer mudah alih persendirian untuk tugas rasmi mestilah mendapat kelulusan bertulis daripada Ketua Jabatan dan perlu disemak serta diperbaharui kelulusan tersebut setiap (1) tahun.

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 diguna pakai 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 storan) dan manusia. Dasar ini adalah terpakai oleh semua warga 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, mengemas kini, 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 maklumat / data.

d. Pengauditan Keselamatan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti 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. 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 ketersediaan, kebolehcapaian dan kerahsiaan. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan melalui pendekatan seperti berikut:

i. Pelan Pemulihan Bencana Sistem ICT hendaklah disedia dan 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.

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:

i. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.
ii. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
iii. Melaksanakan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing. Bahagian Teknologi Maklumat dan Komunikasi Negeri (BTMKN) / Bahagian ICT Jabatan / Agensi Negeri berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Jabatan Negeri/ Agensi berkaitan.
iv. Menguatkuasakan amalan melapor sebarang insiden yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan/ pemulihan.

g. Pengasingan

Pengasingan daripada segi fungsi, proses dan persekitaran operasi pelaksanaan ICT adalah perlu untuk mengekalkan integriti dan perlindungan keselamatan beberapa kesilapan dan penyalahgunaan kuasa. Manakala pengasingan persekitaran adalah perlu untuk pembangunan, pengujian dan pelaksanaan sistem.

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 dalam rangkaian 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 tindakan 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: DASAR KESELAMATAN	
1.1 Pengurusan Keselamatan Maklumat ICT	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Kerajaan Negeri Pulau Pinang.	
1.1.1 Dasar Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dikomunikasikan oleh pihak pengurusan Kerajaan Negeri Pulau Pinang kepada semua pengguna Jabatan/Agensi Negeri (termasuk kakitangan, pembekal, pakar runding dan lain-lain). YB Setiausaha Kerajaan Negeri adalah bertanggungjawab terhadap pelaksanaan dasar ini dengan dibantu oleh Jawatankuasa Pemandu *Electronic Good Governence* yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan Negeri Pulau Pinang.	SUK / Pegawai yang diturunkan kuasa
1.1.2 Kajian Semula Dasar Keselamatan Maklumat	
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 : i. Kenalpasti dan tentukan perubahan yang diperlukan; ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO masing-masing untuk dibentangkan kepada Jawatankuasa CERT Negeri bagi mendapatkan persetujuan Mesyuarat Jawatankuasa Pemandu *Electronic Good Governence (eGG)*; iii. Perubahan yang telah dipersetujui oleh eGG dimaklumkan kepada semua pengguna; dan iv. Dasar ini hendaklah dikaji semula sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa.	Pengurus ICT dan ICTSO
Bidang 02: ORGANISASI KESELAMATAN MAKLUMAT	
2.1 Organisasi Dalaman	
Objektif: 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**.	

2.1.1 Peranan dan Tanggungjawab Organisasi Keselamatan Maklumat	
(a) Setiausaha Kerajaan Negeri (SUK) Peranan dan tanggungjawab SUK adalah seperti berikut : i. Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan ICT bagi semua Jabatan/Agensi Negeri; ii. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan ICT Jabatan/Agensi Negeri; iii. Merancang, menyelaras dan menyeragamkan pelaksanaan program/ projek-projek keselamatan ICT Jabatan/Agensi Negeri supaya selaras dengan Pelan Strategik ICT; iv. Memastikan keperluan sumber bagi keselamatan ICT Jabatan/Agensi Negeri adalah mencukupi; dan v. Memastikan pelaksanaan penilaian risiko keselamatan ICT Jabatan/Agensi Negeri.	SUK
(b) Ketua Pegawai Maklumat (CIO) Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO) di semua Jabatan dan Agensi Negeri adalah seperti berikut : i. Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; ii. Menentukan keperluan keselamatan ICT ; iii. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; iv. Memastikan setiap pegawai dan kakitangan menandatangani surat akuan pematuhan Dasar Keselamatan ICT; v. Mengambil tindakan tatatertib ke atas anggota yang melanggar Dasar Keselamatan ICT Negeri. vi. Menguruskan tindakan ke atas insiden keselamatan yang berlaku sehingga keadaan pulih; vii. Mengaktifkan *Business Resumption Plan* (BRP) jika perlu; dan viii. Menentukan sama ada insiden keselamatan yang berlaku perlu dilaporkan kepada agensi penguatkuasa undang-undang / keselamatan.	CIO

(c) Pegawai Keselamatan ICT (ICTSO) Peranan dan tanggungjawab ICTSO di semua Jabatan/Agensi Negeri yang dilantik adalah seperti berikut: i. Mengurus program-program keselamatan ICT; ii. Menguatkuasakan Dasar Keselamatan ICT; iii. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua pengguna; iv. Mewujudkankan garis panduan, prosedur dan tatacara yang berkaitan selaras dengan keperluan Dasar Keselamatan ICT Negeri; v. Menjalankan pengurusan risiko dan keselamatan ICT; vi. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; vii. Memberi amaran kepada agensi terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; viii. Menentukan tahap keutamaan insiden, melaporkan insiden keselamatan ICT kepada Pasukan CERT NEGERI dan memaklumkan kepada CIO serta mengambil langkah pemulihan awal; ix. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan langkah-langkah baik pulih dengan segera; x. Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Negeri; dan xi. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO
(d) Pengurus ICT Peranan dan tanggungjawab Pengurus ICT adalah termasuk seperti berikut : i. Memastikan kajian semula dan melaksanakan kawalan keselamatan selaras dengan keperluan Kerajaan Negeri; ii. Menentukan kawalan akses semua pengguna terhadap aset ICT; iii. Melaporkan sebarang perkara atau penemuan mengenai	Pengurus ICT

ancaman keselamatan ICT kepada ICTSO; dan iv. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT.	
(e) Pentadbir Sistem ICT Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : i. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; ii. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT; iii. Memantau aktiviti capaian harian pengguna; iv. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; v. Menyimpan dan menganalisis rekod audit trail; dan vi. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	Pentadbir Sistem
(f) Pengguna Dalaman Peranan dan tanggungjawab Pengguna Dalaman adalah seperti berikut : i. Membaca, memahami dan mematuhi DKICT yang berkuat kuasa; ii. Menjaga kerahsiaan maklumat berkaitan penggunaan ICT; iii. Mengikuti dan menghayati program kesedaran keselamatan ICT; iv. Menandatangani Akuan Pematuhan DKICT seperti di LAMPIRAN A atau yang setara dengannya; dan v. Melaporkan aktiviti yang tidak normal berkaitan ICT kepada ICTSO Jabatan/Agensi Negeri.	Pengguna Dalaman
(g) Pengurus Sumber Manusia Peranan dan tanggungjawab Pengurus Sumber Manusia adalah seperti berikut :	Pengurus Sumber Manusia

i. Memaklumkan dasar, polisi, pekeliling dan garis panduan pengurusan sumber manusia berkaitan dengan ICT; ii. Menyediakan khidmat sokongan pentadbiran bagi urusan menyimpan dan menyelenggarakan maklumat pengurusan sumber manusia berkaitan dengan ICT dengan mematuhi peraturan, undang-undang dan polisi yang berkuat kuasa; iii. Memaklumkan sebarang pertukaran, perpindahan, persaraan dan atau penamatan perkhidmatan kakitangan kepada pentadbir sistem ICT; iv. Menyelaras urusan tatatertib dan perkhidmatan sumber manusia; dan v. Menghebahkan dasar, polisi, pekeliling dan garis panduan yang berkaitan dengan perjawatan, penilaian prestasi, kemajuan kerjaya, skim gaji dan perkara-perkara lain yang berkaitan dengan perjawatan.	
(h) Juruaudit Peranan dan tanggungjawab Juruaudit adalah seperti berikut : i. Mengkaji dan menilai kawalan ke atas pematuhan dan pemantauan keselamatan ICT berdasarkan dasar, standard dan prosedur keselamatan maklumat; dan ii. Menilai kawalan pengurusan keselamatan aset ICT.	Juruaudit
(i) Pihak Ketiga Peranan dan tanggungjawab pihak ketiga adalah seperti berikut : i. Menjaga kerahsiaan maklumat berkaitan penggunaan ICT; ii. Menandatangani perakuan pematuhan keselamatan yang ditetapkan oleh Kerajaan Malaysia atau peraturan yang setara/berkaitan yang berkuat kuasa; iii. Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Jabatan/Agensi Negeri; dan iv. Mendapatkan kelulusan untuk menggunakan kemudahan ICT Jabatan/Agensi Negeri.	Pihak ketiga
(j) Jawatankuasa Pemandu eGG Tugas dan Tanggungjawab Jawatankuasa Pemandu Electronic Good Governance (JKP eGG) khusus berkaitan dengan aspek keselamatan ICT adalah seperti berikut :	JKP eGG

i. Merangka dasar, hala tuju, garis panduan dan piawaian keselamatan ICT; ii. Meneliti, meluluskan dan menguatkuasakan dasar keselamatan ICT; iii. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT; iv. Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan ICT; v. Meneliti dan meluluskan inisiatif untuk peningkatan keselamatan ICT; vi. Memantau ancaman-ancaman utama terhadap aset-aset ICT; dan vii. Memastikan pengauditan sistem ICT dilaksanakan sekurang kurangnya sekali setahun.	
(k) 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: i. Pengurus Bahagian Teknologi Maklumat dan Komunikasi Negeri (BTMKN) – Pengerusi ii. Pegawai Teknologi Maklumat (Kanan), Unit Keselamatan dan Pangkalan Data BTMKN iii. Pegawai Teknologi Maklumat (Kanan), Unit Operasi, Rangkaian dan Sokongan Teknikal BTMKN iv. Pegawai Teknologi Maklumat (Kanan), Unit Pembangunan Sistem dan Portal BTMKN v. Wakil Jabatan Kewangan Negeri vi. Wakil Pejabat Tanah dan Galian Negeri vii. Wakil Jabatan Agama Islam Pulau Pinang viii. Wakil PEGIS ix. Wakil Pejabat Daerah dan Tanah seluruh Pulau Pinang x. Wakil Perpustakaan Negeri Pulau Pinang xi. Wakil Jabatan Perancang Bandar dan Desa xii. Wakil Jabatan Kehakiman dan Syariah Negeri xiii. Wakil Jabatan Kebajikan Masyarakat xiv. Urusetia –BTMKN Tugas dan tanggungjawab Jawatankuasa ini adalah seperti berikut:	CERT Negeri

i. Menilai aspek-aspek teknikal berhubung inisiatif dan projek keselamatan ICT. ii. Memberi nasihat teknikal kepada Jawatankuasa Pemandu eGG. iii. Menyediakan pelan tindakan untuk pembangunan dan peningkatan keselamatan sistem ICT. iv. Menilai pilihan teknologi dan cadangan penyelesaian terhadap keperluan keselamatan sistem ICT. v. Mengkaji semula Dasar Keselamatan ICT dari semasa ke semasa untuk dibentangkan kepada JK Pemandu eGG. **(I) CERT Agensi** Keahlian Jawatankuasa CERT Agensi ditentukan oleh Agensi masing-masing berpandukan kepada Pekeliling Am Bil 4 Tahun 2006 dan pekeliling-pekeliling yang berkaitan.	CIO & JK CERT Agensi
2.1.2 Pengasingan Tugas	
Pengasingan tugas adalah bagi mengurangkan peluang untuk perubahan oleh orang tidak dibenarkan atau tanpa sengaja terhadap aset ICT. Perhatian perlu diberikan agar tiada individu tertentu dalam organisasi yang boleh mencapai, mengubah suai atau menggunakan aset ICT tanpa sebarang kawalan atau pengesanan.	Pengurus ICT dan ICTSO
2.1.3 Hubungan Dengan Pihak Berkuasa	
Organisasi perlu mempunyai hubungan baik dengan semua pihak berkuasa. Jabatan / Agensi Negeri perlu mempunyai kaedah untuk menghubungi semua pihak berkuasa dengan segara apabila berlaku kecemasan.	CIO
2.1.4 Hubungan Dengan Pasukan Pakar (*special interest group*)	
Organisasi perlu mempunyai hubungan baik dengan kumpulan pakar terutamanya berkaitan dengan sistem pengoperasian dan peralatan keselamatan ICT yang digunakan. Jabatan / Agensi Negeri perlu memastikan semua sistem pengoperasian dan peralatan keselamatan ICT yang digunakan	Pengurus ICT

masih disokong dan mempunyai pegawai yang boleh menguruskannya.	
2.1.5 Keselamatan Maklumat Dalam Pengurusan Projek	
Keselamatan maklumat perlu dibincangkan dalam pengurusan projek. Jabatan / Agensi Negeri perlu memastikan semua prosedur keselamatan maklumat dipatuhi dalam melaksanakan sebarang projek.	JK Pemandu Projek
2.2 *Mobile Devices and Teleworking*	
Objektif : Menerangkan kaedah dan keperluan bagi memastikan keselamatan capaian ke rangkaian komputer jabatan secara maya dan penggunaan peranti mudah alih.	
2.2.1 Polisi Peranti Mudah Alih	
Penggunaan telefon pintar, iPad, *tablet* dan *notebook* milik peribadi oleh seluruh anggota pentadbiran Kerajaan Negeri Pulau Pinang untuk mencapai maklumat jabatan adalah tertakluk kepada Polisi dan Garis Panduan *Bring Your Own Device* (BYOD) yang dikuatkuasakan oleh Kerajaan Negeri Pulau Pinang. Garis Panduan yang dikuat kuasa perlu menggariskan tatacara penggunaan secara selamat semua peranti mudah alih supaya selaras dengan prinsip *Confidentiality, Integrity* dan *Availability* (CIA). Pengguna bertanggung jawab untuk memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD dilaksanakan dan diberi perhatian sewajarnya. Tujuan garis panduan BYOD adalah seperti berikut : a. Mengelak risiko kebocoran maklumat rasmi; b. Mengelakkan ancaman risiko keselamatan ke atas infrastruktur ICT; c. Memastikan produktiviti penjawat awam tidak terjejas dalam menjalankan urusan rasmi jabatan; dan d. Meningkatkan integriti data.	Semua anggota pentadbiran Kerajaan Negeri
2.2.2 Capaian Ke Rangkaian Komputer Jabatan Secara Maya	
Capaian ke rangkaian komputer jabatan secara maya hanya dibenarkan kepada pagawai-pegawai di Jabatan dan Badan	Semua anggota pentadbiran

Berkanun Negeri yang perlu menggunakan sistem-sistem dalaman bagi melaksanakan tugas hakiki daripada luar pejabat atau daripada luar rangkaian Penang*EG. Peralatan yang digunakan untuk capaian secara maya adalah tertakluk sepenuhnya kepada keperluan dan tatacara keselamatan ICT yang dinyatakan dalam DKICT ini.	Kerajaan Negeri & Badan Berkanun Negeri
Bidang 03: KESELAMATAN SUMBER MANUSIA	
3.1 Sebelum Perkhidmatan	
Objektif : Memastikan kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab serta peranan masing-masing.	
3.1.1 Penilaian / Tapisan	
Tapisan keselamatan untuk calon kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan perlu dilaksanakan berasaskan keperluan perundangan, peraturan dan etika yang terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Semua
3.1.2 Terma Dan Syarat Pelantikan	
Terma dan syarat perkhidmatan dengan kakitangan dan kontraktor yang dilantik perlu menjelaskan tanggungjawab mereka dan tanggungjawab organisasi berkaitan dengan keselamatan maklumat yang sedang berkuat kuasa.	Semua
3.2 Dalam Perkhidmatan	
Objektif : Memastikan kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan menyedari dan memenuhi keperluan tanggungjawab keselamatan maklumat mereka.	
3.2.1 Tanggungjawab Pengurusan	
Pihak pengurusan perlu memastikan semua kakitangan Jabatan/Agensi Negeri dan pihak ketiga yang berkepentingan : a. Menguruskan keselamatan maklumat berdasarkan perundangan dan peraturan yang berkuat kuasa; b. Mempunyai tahap kesedaran, pengetahuan dan kemahiran mengenai keselamatan maklumat pada tahap yang baik; c. Menandatangani atau memperakukan Pematuhan Dasar Keselamatan ICT sekali setiap tahun; dan d. Disediakan dengan saluran pelaporan pelanggaran polisi dan	Pihak Pengurusan dan ICTSO

prosedur berkaitan dengan keselamatan maklumat.	
3.2.2 Kesedaran, Pendidikan dan Latihan Keselamatan Maklumat	
Semua kakitangan Jabatan/Agensi Negeri dan pihak ketiga yang berkepentingan perlu; a. Mengikuti latihan serta program kesedaran yang berkaitan dengan pengurusan keselamatan ICT dan sekiranya perlu kepada pihak ketiga dari semasa ke semasa; dan b. Memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Pihak Pengurusan
3.2.3 Tindakan Disiplin	
Proses tindakan disiplin dan / atau undang-undang yang formal perlu ada dan dimaklumkan kepada kakitangan Jabatan/Agensi Negeri dan pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh Jabatan/Agensi Negeri.	Pengurus Sumber Manusia
3.3 Penamatan Dan Penukaran Lantikan	
Objektif : Bagi melindungi kepentingan organisasi dalam proses pertukaran atau penamatan perkhidmatan.	
3.3.1 Tanggungjawab Penamatan dan Penukaran Lantikan	
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; b. Menyalurkan maklumat pembatalan 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 kepada Pentadbir Sistem ICT; dan c. Pegawai / kakitangan menandatangani perakuan Akta Rahsia Rasmi 1972 apabila meninggalkan Perkhidmatan Kerajaan.	Pengurus Sumber Manusia

Bidang 04: PENGURUSAN ASET	
4.1 Akauntabiliti / Tanggungjawab Aset	
Objektif : Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.	
4.1.1 Inventori Aset	
Ketua Jabatan bertanggungjawab memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a. Semua aset ICT hendaklah diuruskan mengikut tatacara pengurusan aset alih. b. Semua aset ICT mesti dijaga dengan rapi bagi menjamin keselamatannya daripada kecurian/kerosakan dan perlu mendapat kebenaran bertulis Ketua Jabatan untuk dibawa keluar sekiranya ada maklumat terperingkat.	Ketua Jabatan
4.1.2 Pemilik Aset	
Setiap pengguna aset ICT perlu; a. Memastikan semua aset didaftarkan; b. Menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna; c. Bertanggung jawab sepenuhnya ke atas aset ICT dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; d. Bertanggungjawab di atas kerosakan atau kehilangan aset ICT di bawah kawalannya; e. Melindungi aset ICT daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; f. Melaporkan sebarang kerosakan aset ICT kepada Pentadbir ICT jabatan untuk dibaik pulih; g. Memastikan semua aset ICT dalam keadaan ‘OFF’ apabila meninggalkan pejabat; h. Melaporkan penyelewengan atau salah guna aset ICT kepada ICTSO jabatan. i. Melaporkan dengan menguruskan kehilangan aset ICT mengikut tatacara kehilangan aset alih.	Pegawai Aset ICT

4.1.3 Kegunaan Aset Yang Dibenarkan	
Semua aset ICT yang dibekalkan hendaklah; a. 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; b. Bagi peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; dan c. Dikendalikan dengan mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa.	Semua
4.1.4 Pemulangan Aset	
a. Aset ICT perlu dipulangkan kepada bahagian yang menguruskan aset ICT sekiranya pengguna meninggalkan jawatan yang disandang atau meninggalkan jabatan (bertukar, bersara atau tamat perkhidmatan) daripada Jabatan/Agensi Negeri atau kontrak perjanjian tamat. b. Aset ICT yang perlu dipulangkan kepada pihak ketiga perlu mendapat kelulusan Pegawai Aset ICT Jabatan dan direkodkan bagi tujuan pemantauan; c. Semua maklumat yang disimpan dalam aset ICT yang perlu dipulangkan kepada pihak ketiga perlu disalin keluar atau dihapuskan sebelum pemulangan.	Semua
4.2 Klasifikasi Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
4.2.1 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.	Ketua Jabatan, CIO dan Pegawai ICT

4.2.2 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dilaksanakan mengikut klasifikasi maklumat yang diguna pakai oleh Jabatan/Agensi Negeri.	Ketua Jabatan, CIO dan Pegawai ICT
4.2.3 Pengendalian Maklumat	
Aktiviti pengendalian makumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; e. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan f. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Ketua Jabatan, CIO dan Pegawai ICT
4.3 Pengendalian Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
4.3.1 Pengurusan Media Mudah Alih (*Removal Media*)	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja dan merekodkan penggunaanya; b. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; c. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan d. Menyimpan semua media di tempat yang selamat.	CIO, Pegawai ICT dan Pengguna

4.3.2 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dari Pegawai Aset ICT dan mengikut prosedur Pelupusan Media dan selaras dengan tatacara pelupusan aset alih. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran Ketua Jabatan/Agensi Negeri.	CIO, Pegawai ICT dan Pengguna
4.3.3 Pemindahan Media Fizikal	
Jabatan / Agensi Negeri hendaklah memastikan media yang mengandungi maklumat rasmi dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pengangkutan / penghantaran. Sekiranya maklumat sulit pada media tidak dapat dibuat penyulitan, perlindungan fizikal tambahan pada media wajar dipertimbangkan.	CIO, Pegawai ICT dan Pengguna
Bidang 05: KAWALAN AKSES	
5.1 Keperluan Kawalan Capaian	
Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan ICT dalam mengawal capaian ke atas maklumat.	
5.1.1 Dasar Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Setiap keperluan akses mestilah dirancang, didokumentasikan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada.	ICTSO, Pengurus ICT dan Pentadbir ICT
5.1.2 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian Jabatan/Agensi Negeri, rangkaian agensi lain dan rangkaian awam;	ICTSO, Pengurus ICT dan Pentadbir ICT

b. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
5.2 Pengurusan Capaian Pengguna	
Objektif: Memastikan kawalan capaian oleh pengguna yang dibenarkan sahaja.	
5.2.1 Pendaftaran dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian dikuatkuasakan. Perkara-perkara berikut hendaklah dipatuhi: a. Setiap pengguna mempunyai akaun ID yang unik dan bertanggungjawab terhadap tindakan sendiri. Perkongsian ID adalah tidak dibenarkan; b. Akaun ID pengguna dibatalkan / dihapuskan jika berhenti / bersara / bertukar organisasi; c. Tiada pertindihan akaun ID pengguna.	ICTSO, Pengurus ICT dan Pentadbir ICT
5.2.2 Semakan Akses Pengguna (*Provisioning*)	
Proses semakan akses penguna perlu dilaksanakan dari semasa ke semasa untuk mengkaji semula kebenaran dan pembatalan capaian penguna ke atas aplikasi dan perkhidmatan.	Pentadbir Sistem
5.2.3 Pengurusan *Priviledge Access Rights*	
Penggunaan *Priviledge Access Rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
5.2.4 Pengurusan Kata Laluan Pengguna	
Peruntukan kata-laluan perlu melalui beberapa proses pengurusan yang formal seperti berikut; a. Pengguna perlu menandatangani Surat Akuan Pematuhan DKICT Negeri. b. Pengguna perlu disediakan dengan kata laluan sementara, yang perlu ditukar pada penggunaan pertama;	Pentadbir ICT

c. Prosedur perlu diwujudkan untuk mengesahkan identiti pengguna sebelum menyediakan kata laluan yang baharu, penggantian atau sementara; d. Kata laluan sementara perlu diedar kepada pengguna dengan selamat dimana katalaluan tidak boleh diedarkan kepada pihak ketiga dan dalam *clear text*; e. Kata laluan sementara yang dicipta hendaklah unik dan sukar untuk dianggar; f. Pengguna perlu mengesahkan penerimaan kata laluan; dan g. Kata laluan *default* perlu diubah selepas pemasangan sistem atau perisian.	
5.2.5 Kajian Semula Hak Capaian Pengguna	
Pemilik aset ICT hendaklah mengkaji semula hak capaian pengguna secara berkala atau sekurang-kurangnya satu (1) kali setahun.	Pentadbir ICT, Pengurus ICT dan ICTSO
5.2.6 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data dan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku sebarang perubahan. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. Jabatan/Agensi Negeri boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib.	Pentadbir ICT, Pengurus ICT dan ICTSO
5.3 Tanggungjawab Pengguna	
Objektif: Untuk memastikan pengguna bertanggungjawab melindungi maklumat yang digunakan untuk pengesahan identiti mereka.	
5.3.1 Penggunaan Kata Laluan	
Setiap pengguna sistem ICT mestilah mempunyai id pengguna (*user id*) dan kata laluan (*password*) masing-masing dan; a. Bertanggungjawab terhadap kata laluan masing-masing agar tidak berlaku kebocoran kepada orang lain; b. Penggunaan teknologi tambahan seperti kad-kad pintar dan	Pengguna, Pentadbir ICT, Pengurus ICT dan ICTSO

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 jika penggunaannya melanggar peraturan.	
5.4 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
5.4.1 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir ICT, Pengurus ICT dan ICTSO
5.4.2 Prosedur *Log On*	
Capaian kepada sistem dan aplikasi hendaklah dikawal oleh prosedur *log on* mengikut keperluan. BTMKN hendaklah mengenal pasti teknik pengesahan *log on* yang sesuai iaitu : a. Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sah; b. Tidak memberikan bantuan mesej semasa prosedur *log on*; c. Pengesahan *log on*; d. Perlindungan terhadap *Brute Force log on*; e. Log “aktiviti *log on*” yang berjaya dan tidak berjaya; f. Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan *log on* berjaya dikesan; g. Tidak memaparkan kata laluan; h. Tidak menghantar kata laluan dalam *clear-text* melalui rangkaian; dan i. Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu.	Pentadbir ICT, Pengurus ICT dan ICTSO

5.4.3 Sistem Pengurusan Kata Laluan	
Sistem pengurusan kata laluan mestilah interaktif dan menjamin kata laluan yang berkualiti seperti berikut; a. Pengguna boleh menukar kata laluan sendiri; b. Kata laluan perlu ditukar secara berkala; c. Tidak memaparkan kata laluan pada skrin; d. 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.	Pentadbir ICT, Pengurus ICT dan ICTSO
5.4.4 Pengunaan Sistem Utiliti	
Penggunaan program utiliti yang mungkin boleh *Over-Riding System* perlu dihadkan hanya kepada Pentadbir Sistem ICT dan dikawal ketat penggunaannya.	Pentadbir ICT, Pengurus ICT dan ICTSO
5.4.5 Kawalan Akses Kepada Kod Sumber (*Source Code)*	
Pembangunan aplikasi/sistem di Jabatan / Agensi Negeri perlu diluluskan oleh Jawatankuasa Permohonan Projek ICT dan dipantau oleh BTMKN atau pegawai yang bertanggungjawab terhadap aplikasi/sistem berkenaan. Selain itu, semua kod sumber aplikasi/sistem adalah tertakluk kepada perkara seperti berikut; a. Kakitangan sokongan Jabatan / Agensi Negeri perlu dihadkan akses kepada kod sumber; b. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan yang ketat; dan c. Kod sumber bagi semua aplikasi dan perisian adalah hak milik Kerajaan. d. Sekiranya perlu, kod sumber perlu diasingkan daripada *production server*.	Pentadbir ICT, Pengurus ICT dan ICTSO
Bidang 06 : KRIPTOGRAFI	
6.1 Kawalan Penyulitan Maklumat (*Cryptography*)	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	

6.1.1 Polisi Pengunaan Penyulitan Maklumat	
Perkara-perkara berkaitan penyulitan maklumat yang perlu dipatuhi adalah seperti berikut; a. Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah penyulitan yang sesuai pada setiap masa; b. Mengenal pasti tahap perlindungan pengunaan penyulitan dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan; dan c. 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, *Mobile Network* dan sebagainya).	Semua Pengguna dan Pentadbir ICT
6.1.2 Pengurusan Kunci Penyulitan (*Key Management*)	
Kunci penyulitan perlu diuruskan dengan baik, iaitu; a. Diuruskan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; dan b. Peralatan yang digunakan untuk menjana, menyimpan dan arkib kunci penyulitan perlu dilindungi secara fizikal. c. Sistem pengurusan kunci perlu berdasarkan satu set piawaian, prosedur dan kaedah yang dipersetujui.	Semua Pengguna dan Pentadbir ICT
Bidang 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN	
7.1 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal tanpa kebenaran yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat.	
7.1.1 Kawalan Kawasan	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk akses, merosakkan atau mengganggu 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	Semua Pengguna dan BKP

bergantung kepada keperluan untuk melindungi aset dan berdasarkan kepada hasil penilaian risiko; b. Mewujudkan 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; dan i. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan.	
7.1.2 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Jabatan / Agensi Negeri. Perkara yang perlu dipatuhi adalah seperti berikut; a. Setiap pegawai dan kakitangan hendaklah mempamerkan Pas Keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan apabila bertukar, tamat perkhidmatan atau bersara; b. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan c. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT Jabatan / Agensi Negeri.	Semua Pengguna dan BKP
7.1.3 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut; a. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh pihak luar; b. Pegawai pengiring perlu sentiasa berada bersama pihak vendor sekiranya perlu melaksanakan tugas di Pusat Data; dan c. Penunjuk ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	

7.1.4 Perlindungan Terhadap Ancaman Luaran dan Dalaman	
Jabatan / Agensi Negeri perlu merekabentuk dan melaksanakan perlindungan fizikal yang sewajarnya daripada ancaman kebakaran, banjir, letupan, kacau bilau dan bencana.	BKP
7.1.5 Kawalan Tempat Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang diberi kebenaran sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan yang dimaksudkan adalah Pejabat Operasi ICT Jabatan / Agensi Negeri, Bilik Server, Pusat Data (*Data Centre*) dan Pusat Pemulihan Bencana (DRC). Perkara yang perlu dipatuhi adalah seperti berikut: a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Pihak lain adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali dengan kebenaran khas Jabatan / Agensi Negeri dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; b. Pelaksanaan kerja oleh kontraktor tanpa pengawasan pegawai bertugas di kawasan larangan harus dielakkan; c. Bilik dalam kawasan larangan perlu dikunci pada setiap masa; d. Fotografi, video, audio atau peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran; dan e. Pengguna Jabatan / Agensi Negeri dan pengguna luar yang perlu berurusan di bilik server, pusat data dan DRC hendaklah memaklumkan kepada Pentadbir Pusat Data terlebih dahulu dengan mengisi borang permohonan memasuki Pusat Data / DRC dan mengisi buku log keluar masuk Pusat Data / DRC.	Semua Pengguna, ICTSO dan BKP
7.1.6 Kawasan Penghantaran dan Pemunggahan	
Jabatan / Agensi Negeri hendaklah memastikan kawasan-kawasan penghantaran, pemunggahan dan tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Semua Pengguna, ICTSO dan BKP
7.2 Keselamatan Peralatan ICT	
Objektif: Melindungi peralatan ICT Jabatan / Agensi Negeri daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	

7.2.1 Kedudukan dan Kawalan Peralatan ICT	
Sub bidang 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 : a. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b. 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; c. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; d. Pengendalian peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; e. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; f. Memastikan semua perkakassan komputer, pencetak dan pengimbas dalam keadaan 'OFF' apabila meninggalkan pejabat; dan g. Menutup suis dan menanggalkan palam kuasa bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	Semua Pengguna dan ICTSO
7.2.2 Alat Sokongan	
a. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b. Peralatan sokongan seperti UPS dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua alat sokongan perlu disemak dan diuji secara berjadual bagi memastikan ia dapat berfungsi dengan baik.	Semua Pengguna dan ICTSO
7.2.3 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan	Pentadbir Pusat

data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. 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.	Data
7.2.4 Penyelenggaraan Peralatan	
Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Semua Pengguna dan Pegawai Aset ICT
7.2.5 Peralatan Dibawa Keluar Premis	
Peralatan ICT yang hendak dibawa keluar daripada premis Jabatan / Agensi Negeri untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa mempunyai tempoh had masa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pegawai Aset ICT dan Ketua Jabatan
7.2.6 Keselamatan Peralatan di Luar Premis	
Peralatan yang dibawa keluar daripada premis Jabatan / Agensi Negeri adalah terdedah kepada pelbagai risiko. Perkara-perkara yang	Semua Pengguna,

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.	Pegawai Aset ICT
7.2.7 Pelupusan Peralatan dan Kitar Semula	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan / Agensi Negeri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan / Agensi Negeri. Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui kaedah atau teknik yang bersesuaian agar maklumat tidak dapat dicapai semula; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat pendua (salinan maklumat); c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti 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 menjamin keselamatan peralatan tersebut; f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset; g. Pelupusan peralatan ICT hendaklah dilaksanakan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana	Semua Pengguna, Pegawai Aset ICT dan Ketua Jabatan

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 kerana kerja-kerja pelupusan adalah di bawah tanggungjawab Jabatan / Agensi Negeri.	
7.2.8 Penjagaan Peralatan Yang Tidak Diguna	
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a. Tamatkan sesi aktif apabila selesai tugas; b. Log-off server, log keluar daripada aplikasi dan PC pejabat serta apabila sesi bertugas selesai; dan c. Kawal keselamatan komputer dan peralatan mudah alih daripada akses yang tidak dibenarkan dengan menggunakan katalaluan, *lock screen* dan sebagainya apabila tidak digunakan.	Semua Pengguna
7.2.9 *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 Scree*n bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan password *screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif seperti media storan dan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci; c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat; d. E-mel masuk dan keluar hendaklah dikawal; dan e. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Semua Pengguna

Bidang 08 : KESELAMATAN OPERASI	
8.1 Pengoperasian dan Tanggungjawab	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas fasiliti pemprosesan maklumat.	
8.1.1 Dokumentasi Prosedur Pengoperasian	
Bagi memastikan prosedur pengoperasian didokumentasikan dan disediakan untuk pengguna-pengguna yang berkaitan perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah 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.	Pengurus ICT dan ICTSO
8.1.2 Pengurusan Perubahan	
Perubahan terhadap organisasi, proses, operasi, sistem dan fasiliti pemprosesan maklumat yang memberi kesan terhadap keselamatan maklumat perlu dikawal. Oleh itu, perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Ketua Jabatan /Agensi Negeri atau Pengurus ICT; 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; c. Semua aktiviti pengubahsuaian komponen peralatan ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua Pengguna dan Pengurus ICT

8.1.3 Pengurusan Kapasiti	
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem, Pentadbir Pusat Data dan Pengurus ICT
8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
a. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi perlu diasingkan dari perkakasan sebenar yang digunakan (*production*) bagi mengurangkan risiko. b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem dan Pengurus ICT
8.2 Perlindungan daripada *Malware*	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
8.2.1 Kawalan daripada Perisian Berbahaya	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini anti virus dengan paten antivirus yang terkini, pengemaskinian perlu dilakukan sekurang-kurangnya sekali sehari atau apabila terdapat paten terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;	Semua Pengguna, Pentadbir Sistem dan ICTSO

f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya; h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; i. Memaklumkan sebarang peringatan / amaran / ancaman / kerosakan yang dikesan kepada Pentadbir Sistem / ICTSO; dan j. Mengambil tindakan yang sewajarnya terhadap semua peringatan / arahan yang dikeluarkan oleh Pentadbir Sistem / ICTSO.	
8.3 *Backup*	
Objektif: Melindungi daripada kehilangan data.	
8.3.1 *Backup* Maklumat	
Bagi memastikan sistem dapat diaktifkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut: a. Salinan direkodkan dan di simpan di *off-site*. Lokasi *off-site* tidak boleh di bangunan yang sama dan pemilihan lokasi mestilah praktikal dengan mengambil kira aspek geografi, kemudahan, keselamatan, kos dan persekitaran; b. Salinan dilakukan setiap kali konfigurasi berubah. Kekerapan salinan dilakukan bergantung pada tahap kritikal maklumat; c. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; d. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; e. Menyimpan sekurang-kurangnya tiga (3) generasi salinan penduaan; dan f. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Semua Pengguna, Pentadbir Sistem

8.4 Log dan Pemantauan	
Objektif: Merekodkan peristiwa dan menjana bukti.	
8.4.1 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti penguna Jabatan / Agensi Negeri yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu peristiwa. 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 ICT dan personel keselamatan sahaja; c. Aktiviti-aktiviti Pentadbir Sistem ICT mestilah dilogkan; d. Sebarang cubaan memasuki sistem *(login)* yang tidak berjaya mestilah dilogkan dan perlu diberi perhatian; e. Penggera keselamatan boleh dipertimbangkan untuk memberikan amaran kepada Pentadbir Sistem ICT secara automatik sebagai tanda peringatan; dan f. Semua sistem komputer dan peranti rangkaian mestilah mempunyai catatan masa yang seragam bagi memastikan kesahihan masa yang tercatat dalam log audit. g. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan h. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada Pegawai Keselamatan Teknologi Maklumat (ICTSO) dan CIO.	Semua Pengguna, Pentadbir Sistem, Pentadbir Rangkaian dan ICTSO
8.4.2 Perlindungan Maklumat Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.	
8.4.3 Log Pentadbir dan Operator	
a. Pentadbir Sistem ICT dan Pentadbir Rangkaian dikehendaki menganalisa log/audit *trail* dari semasa ke semasa; b. Aktiviti pentadbir dan pengendali sistem perlu direkodkan; dan	Pentadbir Sistem, Pentadbir

c. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu.	Rangkaian dan ICTSO
8.4.4 Penyelarasan Waktu	
a. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan/Agensi Negeri atau perkakasan keselamatan ICT perlu diselaraskan; dan b. Jabatan / Agensi Negeri perlu menyediakan NTP Server atau menggunakan mana-mana sumber waktu setempat yang mematuhi *Malaysian Standard Time*.	Pentadbir Sistem
8.5 Kawalan Perisian Operasi	
Objektif: Memastikan integriti sistem yang beroperasi.	
8.5.1 Pemasangan Perisian Pada Sistem Operasi	
a. Pengemaskinian perisian operasi, aplikasi dan *program libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; b. Sistem operasi hanya boleh memegang "*executable code*" dan tidak kod pembangunan atau penyusun; c. Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; d. Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi, konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan; e. Satu "rollback" strategi harus diadakan sebelum perubahan dilaksanakan; f. Versi perisian perlu disimpan sebagai pelan konfigurasi; dan g. Versi lama perisian perlu diarkib bersama dengan maklumat dan parameter, prosedur, maklumat konfigurasi terperinci dan perisian yang menyokongnya selama mana data boleh disimpan di dalam arkib (*archive*).	Pentadbir Sistem & Pengurus ICT
8.6 Pengurusan Keterdedahan Teknikal	
Objektif: Memastikan pengurusan keterdedahan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	

8.6.1 Pengurusan Kelemahan Teknikal	
Kawalan dari ancaman teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Organisasi perlu memberi definisi dan tanggungjawab berkaitan pengurusan kelemahan teknikal termasuk pemantauan kelemahan, penilaian risiko kelemahan, paterning, asset tracking dan tanggungjawab koordinasi. b. Memperoleh maklumat keterdedahan teknikal yang tepat pada masanya ke atas sistem maklumat yang digunakan; c. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d. Mengambil langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem dan ICTSO
8.6.2 Kawalan Pemasangan Perisian	
a. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. b. Selain daripada perisian automasi pejabat yang ditetapkan oleh jabatan, pengguna perlulah mendapatkan kebenaran daripada pemilik aset ICT terlebih dahulu; dan c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya.	Semua Pengguna, Pentadbir Sistem dan ICTSO
8.7 Pertimbangan Pelaksanaan Audit Sistem Maklumat	
Untuk meminimakan impak aktiviti audit terhadap sistem pengoperasian.	
8.7.1 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	
a. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlakunya gangguan dalam penyediaan perkhidmatan. b. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan. c. Pelaksanaan audit keatas sistem pengoperasian dilaksanakan sekurang-kurangnya setahun sekali. d. Ujian audit perlu diberi akses terhad kepada *read only* akses pada perisian dan data. e. Jabatan / Agensi Negeri memohon perkhidmatan audit sistem maklumat daripada unit keselamatan PSUKPP. f. Pentadbir Sistem perlu mengambil tindakan keatas penemuan audit yang berstatus '*Critical*' dan '*High*'.	ICTSO dan Audit Dalaman

Bidang 09 : PENGURUSAN KOMUNIKASI	
9.1 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan perlindungan maklumat dalam rangkaian dan fasiliti yang membantu pemprosesan maklumat.	
9.1.1 Kawalan Infrastruktur Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: a. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. Firewall hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan Jabatan / Agensi Negeri; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO); h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Jabatan / Agensi Negeri; i. Memasang *Web Content Filtering* pada Internet Gateway bagi menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan / Agensi Negeri adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di Jabatan / Agensi Negeri sahaja dan penggunaan modem adalah dilarang sama sekali; l. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; m. Semua perjanjian perkhidmatan rangkaian hendaklah	Semua Pengguna, Pentadbir Rangkaian dan ICTSO

mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; n. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; o. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; p. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan Jabatan / Agensi Negeri; dan q. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan Jabatan / Agensi Negeri.	
9.1.2 Keselamatan Perkhidmatan Rangkaian	
Semua perkhidmatan rangkaian yang disediakan secara *inhouse* atau *outsourced* perlu dikenal pasti mekanisme keselamatan, pengurusan dan tahap perkhidmatan serta perlu dimasukkan dalam perjanjian perkhidmatan rangkaian.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
9.1.3 Pengasingan rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Jabatan / Agensi Negeri.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
9.2 Pemindahan Maklumat	
Objektif: Menjamin keselamatan perpindahan/pertukaran maklumat dan perisian antara Jabatan/Agensi Negeri dengan pihak luar terjamin.	
9.2.1 Polisi dan Prosedur Pemindahan Maklumat	
Perkara berkaitan dasar dan prosedur pemindahan maklumat yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; b. Terma pemindahan maklumat dan perisian antara Jabatan / Agensi Negeri dengan pihak luar hendaklah dimasukkan dalam Perjanjian; c. Media yang mengandungi maklumat perlu dilindungi daripada	Semua Pengguna, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO

capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan d. Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. e. Merujuk dan melaksanakan dasar yang dilaksanakan dalam Klausa 4.3.3.	
9.2.2 Perjanjian Mengenai Pemindahan Maklumat	
Jabatan/Agensi Negeri perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara Jabatan /Agensi Negeri dengan pihak luar. Perkara yang perlu dipertimbangkan adalah: a. Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi; b. Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat; dan c. Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	CIO dan Pengurus ICT
9.2.3 Pengurusan Mel Elektronik (e-Mel)	
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. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Membaca, memahami dan mematuhi peraturan yang digariskan dalam Polisi e-Mel Rasmi Kerajaan Negeri; b. Pentadbir Sistem ICT perlu memastikan setiap pelayan e-mel dipasang dengan pelayan antivirus e-mel bagi membolehkan pengimbasan dilakukan sebelum e-mel sampai kepada pengguna; c. Penggunaan kemudahan e-mel adalah untuk tujuan perkhidmatan rasmi sahaja; d. Semua pihak bertanggungjawab sepenuhnya terhadap kandungan e-mel dalam akaun masing-masing; 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;	Semua Pengguna

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 dalam setiap e-mel rasmi kerajaan seperti : "DISCLAIMER: This e-mel and any files transmitted with it are intended only for the use of the recipient(s) named above and may contain confidential information. You are hereby notified that the taking of any action in reliance upon, or any review, retransmission, dissemination, distribution, printing or copying of this message or any part thereof by anyone other than the recipient(s) is strictly prohibited. If you have received this message in error, you should delete it immediately and advise the sender by return e-mel. Opinions, conclusions and other information in this message that do not relate to the Penang State Government shall be understood as neither given nor endorsed by the Penang State Government." i. Akaun e-mel yang diberi adalah bukan hak persendirian. Pentadbir Sistem e-Mel berhak mengakses mana-mana akaun bagi tujuan pengurusan akaun e-mel, keselamatan dan undang-undang; j. Elakkan membuka e-mel daripada penghantar yang tidak diketahui dan diragui; k. Mengimbas bahan-bahan yang hendak dimuat naik atau dimuat turun supaya bebas virus sebelum digunakan; l. Semua pihak dilarang daripada melakukan aktiviti yang melanggar tatacara penggunaan e-Mel rasmi kerajaan seperti yang telah digariskan di dalam Polisi e-Mel Rasmi Kerajaan Negeri Pulau Pinang; dan m. Sebarang pelanggaraan polisi penggunaan e-Mel akan dikenakan tindakan seperti yang telah digariskan dalam Polisi e-Mel Rasmi Kerajaan Negeri Pulau Pinang atau mengikut polisi Agensi berkenaan.	
9.2.4 Kerahsiaan dan *Non-Disclosure Agreement*	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure agreement* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari semasa ke semasa.	CIO, Pengurus ICT, Ketua Jabatan / Pengurus Kanan dan ICTSO
Bidang 10 : PEROLEHAN SISTEM, PEMBANGUNAN DAN PENYELENGGARAAN	
10.1 Keperluan Keselamatan Sistem Maklumat	
Objektif: Memastikan keselamatan maklumat merupakan sebahagian daripada proses	

pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Perkara-perkara berkaitan analisis keperluan dan spesifikasi keselamatan maklumat yang perlu dipatuhi adalah sepertiberikut : 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 input sistem untuk menyemak pengesahan dan integriti data yang dimasukkan, pemprosesan sistem untuk menentukan sama ada program berjalan betul serta sempurna dan ujian output sistem adalah 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 luaran hendaklah diuji bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik dan Pentadbir Sistem
10.1.2 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); b. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; c. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT; dan d. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem

10.1.3 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; b. Memastikan semua aspek transaksi dipatuhi: i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan. ii. Mengekalkan kerahsiaan maklumat. iii. Mengekalkan privasi pihak yang terlibat. iv. Komunikasi antara semua pihak yang terlibat dirahsiakan. v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. c. Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem
10.2 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
10.2.1 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan selaras dengan perkembangan dan perubahan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Keselamatan persekitaran pembangunan; b. Panduan keselamatan dalam kitar hayat pembangunan (*development lifecycle*) sistem/aplikasi; c. Keselamatan dalam fasa reka bentuk; d. Pemeriksaan keselamatan dalam perkembangan projek; e. Keselamatan repositori; f. Keselamatan dalam kawalan versi; g. Keperluan pengetahuan keselamatan dalam pembangunan sistem/aplikasi ; dan	Pentadbir Sistem dan ICTSO

h. Kebolehan pembekal untuk mengenal pasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem.	
10.2.2 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumentasi dan disahkan sebelum diguna pakai; b. Setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan agensi; dan c. Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	Pentadbir Sistem dan Pengurus ICT
10.2.3 Kajian Teknikal Selepas Permohonan Perubahan *Platform*	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b. Perubahan platform dimaklumkan dari masa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan c. Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan perkhidmatan Jabatan/Agensi Negeri.	Pentadbir Sistem dan Pengurus ICT
10.2.4 Sekatan Perubahan Pakej Perisian	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem, Pengurus ICT dan ICTSO
10.2.5 Prinsip Kejuruteraan Keselamatan Sistem	
Keselamatan perlu diambil kira dalam semua peringkat pembangunan sistem. Prinsip dan prosedur keselamatan ICT hendaklah sentiasa dikaji dari semasa ke semasa bagi memastikan keberkesanan keselamatan maklumat.	Pentadbir Sistem dan Pengurus ICT

10.2.6 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*).	Pentadbir Sistem dan Pengurus ICT
10.2.7 Pembangunan Sistem Secara *Outsource*	
a. Pembangunan sistem secara *outsource* perlu sentiasa dikawal selia dan dipantau; b. Semua aplikasi dan perisian adalah menjadi hak milik Kerajaan; dan c. *Intellectual property rights* (IPR) aplikasi dan perisian yang dibangun oleh pihak ketiga kepada Jabatan / Agensi Negeri adalah hak milik Kerajaan.	
10.2.8 Pengujian Keselamatan Sistem	
Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan; a. Semua sistem baru dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input and output validation*); b. Menyemak dan mengesahkan data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; c. Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; d. Membuat semakan pengesahan dalam aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan; dan e. Menjalankan proses semak ke atas *output data* daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Pentadbir Sistem dan ICTSO
10.2.9 Penerimaan Pengujian Sistem	
Penerimaan pengujian semua sistem baru dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai.	Pentadbir Sistem dan Pengurus ICT
10.3 Data Ujian	
Objektif : Memastikan data ujian direkod dan diuruskan dengan sewajarnya.	
10.3.1 Perlindungan Data Ujian	
a. Data dan aturcara yang hendak diuji perlu dipilih, dilindungi	Pemilik dan

dan dikawal; b. Pengujian hendaklah dibuat ke atas aturcara yang terkini; dan c. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem
Bidang 11: HUBUNGAN DENGAN PEMBEKAL	
11.1 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan perlindungan aset Jabatan / Agensi Negeri yang boleh diakses oleh pembekal.	
11.1.1 Dasar Keselamatan Maklumat Untuk Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan bersama pembekal bagi mengurangkan risiko terhadap aset Jabatan / Agensi Negeri. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a. Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal; d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; dan g. Keperluan keselamatan ICT jabatan dimaklumkan (*communicate*) kepada pembekal yang dilantik.	Jabatan / Agensi Negeri dan Pembekal
11.1.2 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur dan maklumat organisasi ICT. Perkara-perkara yang perlu diambil kira seperti berikut: a. Penerangan maklumat keselamatan; b. Klasifikasi maklumat; c. Keperluan undang-undang dan peraturan; d. Obligasi setiap pihak bagi kawalan akses, pemantauan,	Jabatan / Agensi Negeri dan Pembekal

pelaporan dan pengauditan; e. Penerimaan peraturan penggunaan maklumat oleh pembekal; f. Kesedaran keselamatan maklumat; g. Tapisan keselamatan pembekal; h. Hak untuk mengaudit pembekal; i. Kewajipan pembekal mematuhi keperluan keselamatan maklumat; j. Menandatangani *Non-Disclosure Agreement* (NDA).	
11.1.3 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk; d. Melaksanakan satu proses/kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat Jabatan / Agensi Negeri; e. Jabatan / Agensi Negeri hendaklah mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan; f. Memastikan jaminan dari pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan g. Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara organisasi dan pembekal.	Jabatan / Agensi Negeri & Pembekal
11.2 Pengurusan Penyampaian Perkhidmatan Pembekal	
Objektif : Memastikan perkhidmatan yang diberikan oleh pembekal adalah pada tahap yang yang terbaik dan berkualiti.	
11.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal	
Jabatan / Agensi Negeri hendaklah sentiasa memantau, mengkaji	Jabatan /

semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c. Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Agensi Negeri & Pembekal
11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal	
Perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh Jabatan/Agensi Negeri bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Jabatan / Agensi Negeri & Pembekal
Bidang 12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT	
12.1 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.	
12.1.1 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	ICTSO, Pengurus ICT dan CERT Negeri
12.1.2 Mekanisme 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	Pengguna, ICTSO dan CERT Negeri

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. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di Negeri Pulau Pinang adalah seperti di **Lampiran 4.**	
12.1.3 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat Jabatan / Agensi Negeri dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT kepada ICTSO Jabatan/Agensi Negeri.	Semua Pengguna
12.1.4 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Sebarang aktiviti yang mengancam keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat ataupun tidak.	ICTSO & CERT Negeri
12.1.5 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b. Menjalankan kajian forensik sekiranya perlu; c. Menghubungi pihak yang berkenaan dengan secepat mungkin; d. Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; e. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;	ICTSO, CERT Negeri dan Pasukan Pemulihan Bencana

g. Menyediakan tindakan pemulihan segera; dan h. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	
12.1.6 Pengalaman Dari Insiden Keselamatan Maklumat	
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 Jabatan / Agensi Negeri.	ICTSO, CERT Negeri dan Pasukan Pemulihan Bencana
12.1.7 Pengumpulan Bahan Bukti	
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, CERT Negeri dan Pasukan Pemulihan Bencana
Bidang 13 : ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
13.1 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Objektif: Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi.	
13.1.1 Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Semua perkhidmatan yang berasaskan ICT terutama proses-proses kritikal perlu disediakan pelan kesinambungan perkhidmatan apabila diperlukan. Ia bertujuan memastikan operasi-operasi di Jabatan/Agensi Negeri berjalan secara berterusan ketika berlaku gangguan atau bencana.	CIO dan Pasukan Pemulihan Bencana

13.1.2 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Jabatan / Agensi Negeri hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara berikut perlu diberi perhatian: a. Struktur pengurusan diwujudkan, mengurus dan memberi respon terhadap situasi bencana menggunakan kakitangan yang berpengalaman, berkompetensi dan mempunyai kuasa; b. Pasukan pemulihan bencana yang mempunyai kompetensi dan kuasa mengendalikan insiden bencana dikenalpasti dan dilantik. c. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; d. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; e. Mendokumentasikan proses dan prosedur yang telah dipersetujui; dan f. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	CIO dan Pasukan Pemulihan Bencana
13.1.3 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Jabatan/Agensi Negeri perlu mengesahkan Pelan Kesinambungan Perkhidmatan (PKP) yang dibangunkan boleh digunapakai dan efektif semasa bencana. Pelan Kesinambungan Perkhidmatan perlu dikaji semula dari semasa ke semasa jika terdapat penambahan organisasi, teknikal dan prosedur. Jabatan/Agensi Negeri perlu mengesahkan PKP dengan: a. Berlatih dan menguji fungsi PKP, proses, prosedur dan kawalan agar konsisten dengan objektif pelan; b. Berlatih dan menguji pengetahuan dalam menguruskan proses, prosedur dan kawalan PKP agar prestasinya konsisten dengan objektif pelan; dan c. Mengkaji semula kesahihan dan keberkesanan pengukuran apabila terdapat perubahan dalam PKP.	CIO, Pasukan Pemulihan Bencana dan ICTSO

13.2 Pertindihan/Duplikasi	
13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat	
Pelan Kesinambungan Perkhidmatan perlu diuruskan secara berikut : a. PKP perlu di simpan di lokasi Pusat Data Utama dan salinannya di Pusat Pemulihan Bencana ICT (Disaster Recovery Centre - DRC) b. Fasiliti DRC perlu diwujudkan bagi memenuhi keperluan semasa; dan c. Fasiliti DRC perlu diuji dari semasa ke semasa.	ICTSO dan Pasukan Pemulihan Bencana
Bidang 14 : PEMATUHAN	
14.1 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak daripada pelanggaran undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
14.1.1 Mengenalpasti Undang-Undang dan Perjanjian Kontrak	
Semua keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan Jabatan / Agensi Negeri perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Perkara berkaitan perundangan yang perlu diberi perhatian adalah seperti berikut: 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 perjanjian dan pekeliling berkaitan 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 Pengguna
14.1.2 Hak Harta Intelek (*Intellectual Property Right*)	
Jabatan / Agensi Negeri mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Jabatan / Agensi	Semua Pengguna

Negeri perlu mematuhi perkara-perkara berikut: a. Keperluan hakcipta yang berkaitan dengan bahan proprietari, perisian, dan rekabentuk perisian atau aplikasi yang dibangunkan oleh Jabatan / Agensi Negeri; b. Keperluan perlesenan menghadkan penggunaan produk, perisian, rekabentuk dan bahan-bahan lain yang diperolehi oleh Jabatan / Agensi Negeri; c. Jabatan / Agensi Negeri perlu memastikan pematuhan berterusan dengan sekatan hakcipta produk dan keperluan perlesenan; dan d. Pengguna tidak dibenarkan daripada menggunakan kemudahan pemprosesan maklumat bagi tujuan selain daripada tugas rasmi atau tugas yang diarahkan.	
14.1.3 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan. Perkara yang perlu ditimbangkan ialah: a. Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; b. Jadual penyimpanan rekod perlu dikenal pasti; dan c. Inventori rekod.	Semua Pengguna
14.1.4 Privasi dan perlindungan maklumat peribadi	
Jabatan / Agensi Negeri perlu mengenal pasti privasi dan melindungi maklumat peribadi penguna seperti yang ditakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Semua Pengguna
14.1.5 Kawalan Kriptografi	
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan enkripsi terhadap penghantaran dokumen / maklumat terperingkat oleh semua pengguna yang berkaitan; dan b. Kaedah akses oleh Jabatan/ Agensi Negeri terhadap maklumat enkripsi bagi perkakasan dan perisian.	Semua Pengguna

14.2 Kajian Keselamatan Maklumat	
Objektif : Bagi memastikan keselamatan maklumat dilaksanakan dan beroperasi bersama-sama polisi dan prosedur organisasi.	
14.2.1 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
Perlaksanaan keselamatan maklumat Jabatan / Agensi Negeri hendaklah dikaji secara bebas atau oleh pihak ketiga secara berjadual berkala bagi mematuhi *standard* pelaksanaan keselamatan ICT.	CIO dan JK ISMS
14.2.2 Pematuhan Dasar dan Standard/Piawaian	
Pengurus perlu membuat kajian semula pematuhan dan prosedur pemprosesan maklumat di bawah tanggungjawab mereka dengan Dasar Keselamatan ICT sedia ada dan piawaian yang berkenaan. Sekiranya kajian semula mengenal pasti ketidakpatuhan, Pengurus perlu: a. Mengenal pasti punca-punca ketidakpatuhan; b. Menilai keperluan tindakan untuk mencapai pematuhan; c. Melaksanakan tindakan pembetulan yang sewajarnya; dan d. Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan.	Ketua Jabatan / Ketua Unit
14.2.3 Pematuhan Kajian Teknikal	
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan *standard* keselamatan maklumat organisasi (contohnya Kajian Security Posture Assessment – SPA). Kajian teknikal perlu dilakukan setahun sekali atau mengikut kesesuaian.	CIO, Ketua Jabatan, ICTSO & Pentadbir ICT

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.

[14] Garis Panduan Keselamatan Dokumen Elektronik Dan Media Storan.

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.
Bring Your Own Device (BYOD)	Garis panduan ini disediakan untuk menggariskan satu tatacara penggunaan secara selamat semua peranti mudah alih supaya selaras dengan prinsip Confidentiality, Integrity dan Availability (CIA).
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 : .....

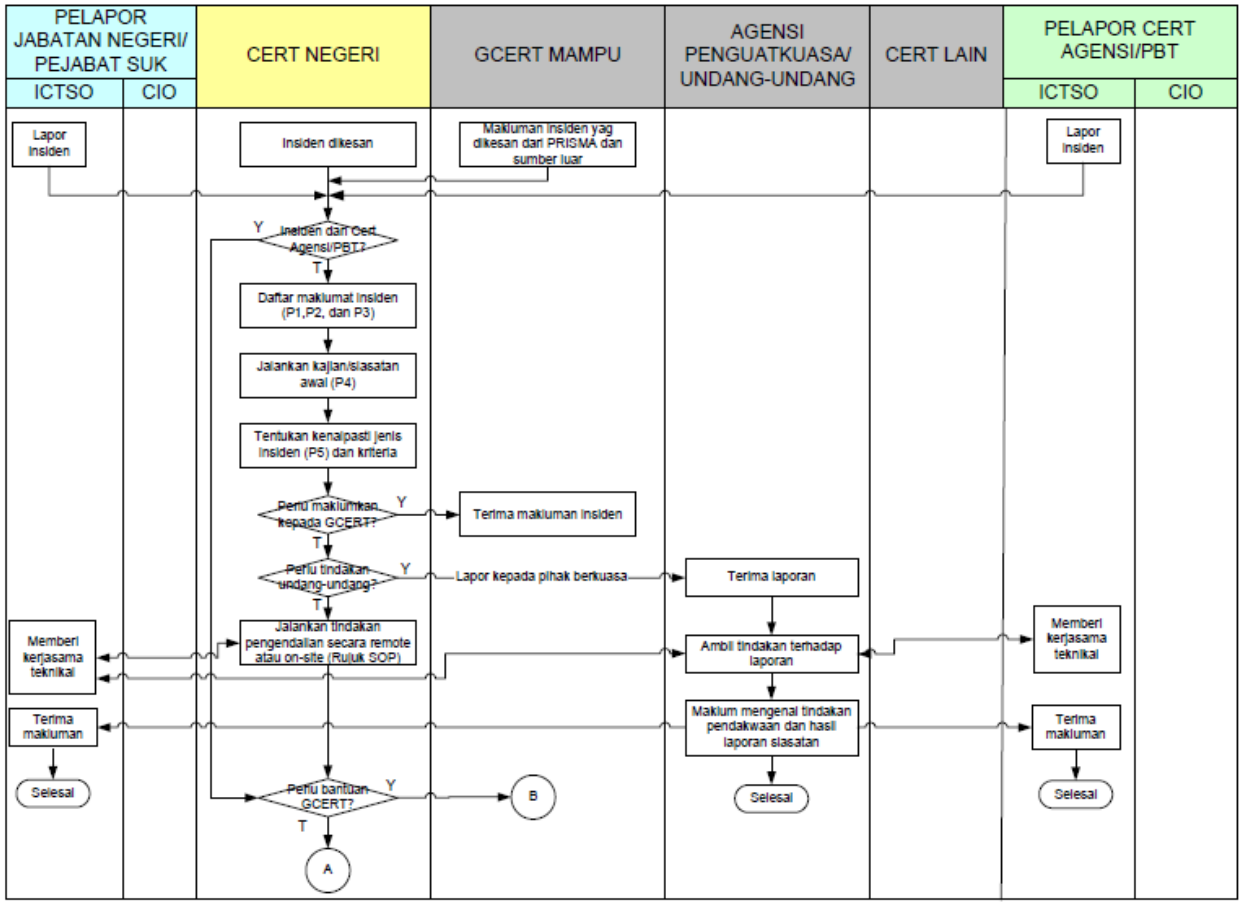
Jabatan/Organisasi:.....

Tarikh:.....

Cop Jabatan/Organisasi:.....

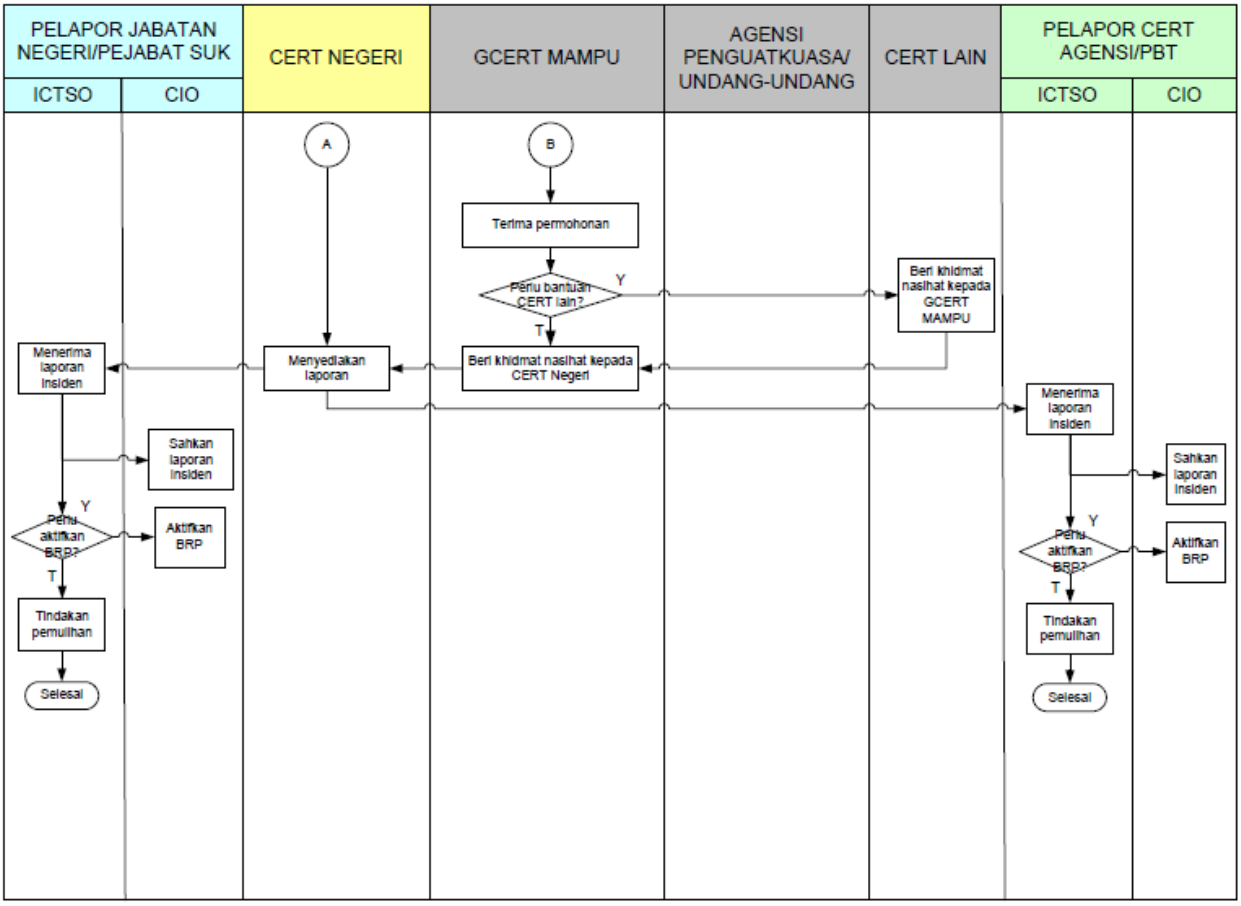
LAMPIRAN 4

RINGKASAN CARTA ALIR PROSES KERJA PENGENDALIAN INSIDEN KESELMATAN ICT CERT NEGERI



LAMPIRAN 4

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 Setiausaha Kerajaan Bil 2 Tahun 2015 Garis Panduan *Bring Your Own Device* Di Pentadbiran Kerajaan Negeri Pulau Pinang.

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

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

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

l. Akta Tandatangan Digital 1997;

m. Akta Jenayah Komputer 1997;

n. Akta Hak cipta (Pindaan) Tahun 1997;

o. Akta Komunikasi dan Multimedia 1998;

p. Perintah-Perintah Am;

q. Arahan Perbendaharaan; dan

r. Arahan Teknologi Maklumat 2007;