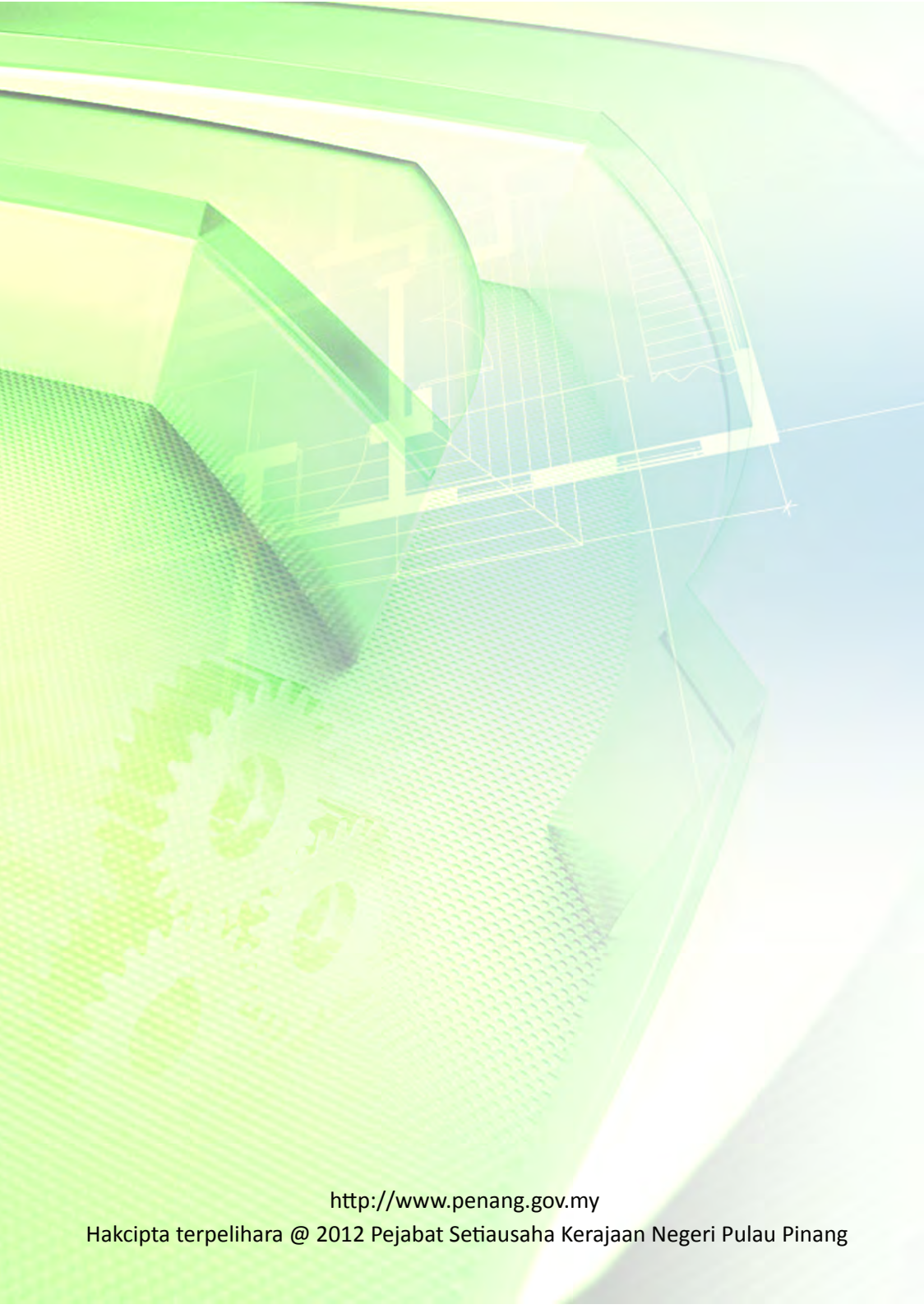


KITBOOK ICTSO

BERSATU DAN SETIA

PANDUAN KESELAMATAN ICT KERAJAAN NEGERI PULAU PINANG

versi 1.0

ISI KANDUNGAN

Nama Undang-Undang	Ringkasan Undang-Undang/URL
	Akta ini seterusnya memperuntukkan: Seksyen 62(2) (a) *A document signed with digital signatures in accordance with this Act shall be legally binding as a document signed with hand-written signatures, an affixed thumb-print or any other marks* (b) *A digital signatures created in accordance with this Act shall be deemed to legally binding signature.*
Akta Teleperubatan 1997	Ringkasan: Akta untuk mengadakan peruntukan bagi pengawalseliaan dan pengawalan amalan teleperubatan dan perkara-perkara yang berkaitan dengannya. Teleperubatan menggunakan ICT dan elektronik bagi pe-nyediaan serta menyokong sektor berkaitan yang bukan sekadar sebagai kegunaan setempat.

Prakata

Y.B. Dato' Farizan Bin Darus

SETIAUSAHA KERAJAAN NEGERI

Bismillahirrahmanirrahim,

Assalamualaikum warahmatullahi wabarakatuh dan Salam Sejahtera.

Peranan Teknologi Maklumat dan Komunikasi (ICT) sebagai mekanisme strategik dalam mempertingkatkan sistem penyampaian perkhidmatan kerajaan amatlah ketara dan memberi impak yang tinggi. Sejajar dengan penggunaan ICT yang meluas di semua peringkat jabatan kerajaan, tadbir urus keselamatan ICT yang berkesan dan mantap menjadi lebih penting. Justeru itu, peranan Pegawai Keselamatan ICT (ICTSO) sebagai penasihat, pelaksana dan penguatkuasa dalam bidang dan aspek keselamatan ICT di peringkat jabatan/agensi negeri amatlah diperlukan.

Alhamdulillah buku ini telah dapat diterbitkan dengan inisiatif Pusat Teknologi Maklumat dan Komunikasi Negeri dengan kerjasama ahli-ahli *Computer Emergency Response Team* (CERT) Negeri Pulau Pinang. Kitbook ICTSO ini meliputi struktur tadbir urus ICTSO dalam bidang berkaitan dasar, pengendalian insiden keselamatan ICT dan perundangan yang berkuatkuasa.

Harapan saya agar kandungan panduan ini difahami oleh semua ICTSO dan seterusnya dimanfaatkan dalam melaksanakan peranan di jabatan/agensi negeri masing-masing.

Sekian, terima kasih.

Prakata

Y.Bhg. Dato' Haji Muhammad Yusof bin Wazir

CHIEF INFORMATION OFFICER (CIO)

Bismillahirrahmanirrahim,

Assalamualaikum warahmatullahi wabarakatuh dan Salam Sejahtera.

Dalam era sains & teknologi ICT yang semakin berkembang pesat dengan kebanyakkan perkhidmatan utama, Kerajaan Negeri Pulau Pinang bergantung sepenuhnya kepada teknologi ICT untuk memenuhi eskpektasi pelanggan yang semakin tinggi dengan pelbagai saluran perkhidmatan disediakan Kerajaan Negeri Pulau Pinang kepada pelanggan. Walaupun begitu seiring dengan kemajuan teknologi ICT juga, isu-isu keselamatan ICT turut meningkat dalam kadar yang membimbangkan dari setahun ke setahun. Untuk menangani isu ini, pihak MAMPU melalui PEKELILING BIL 3 TAHUN 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Negeri telah mewajibkan pihak agensi untuk melantik Pegawai Keselamatan ICT atau lebih dikenali sebagai ICTSO.

Sebanyak 25 orang pegawai daripada jabatan/agensi negeri Pulau Pinang telah dilantik sebagai ICTSO berperanan di dalam memastikan semua aspek berkaitan penguatkuasaan, kawalan dan langkah perlindungan aset ICT kerajaan dipatuhi bagi menjamin kesinambungan perkhidmatan kerajaan dengan meminimumkan kesan insiden keselamatan. Mengambil kira beban semasa, ICTSO yang pada masa yang sama turut perlu melaksanakan kerja-kerja hakiki, Pusat Teknologi Maklumat Dan Komunikasi Negeri (PTMKN) telah mengambil inisiatif menyediakan "Kitbook ICTSO". Kitbook ICTSO ini merupakan kompilasi semua perkara dan maklumat yang perlu diketahui oleh pegawai yang dilantik sebagai ICTSO dan seterusnya membantu memudahkan pelaksanaan tugas.

Akhir kata, saya amat berharap Kitbook ICTSO yang diterbitkan ini dapat memberi manfaat dan berperanan sebagai panduan utama sewaktu menjalankan tugas selaku ICTSO. Adalah menjadi harapan saya supaya "Kitbook ICTSO" ini dapat disemak secara berkala bagi memastikan kandungan yang terdapat di dalamnya relevan dan seiring dengan teknologi semasa. Tahniah di atas usaha dan inisiatif yang diambil untuk menyediakan Kitbook ICTSO".

Sekian, terima kasih.

Nama Undang-Undang	Ringkasan Undang-Undang/URL
	(b) Memindahkan atau menggantikan sebarang hak elektronik maklumat pengurusan tanpa kebenaran (c) Menyebarkan, bermaksud untuk menyebarkan atau menyampaikan kepada orang awam, tanpa kebenaran, bekerja atau menyalin kerja dari sudut yang mana hak elektronik pengurusan maklumat telah dipindahkan atau digantikan tanpa kebenaran. Kesalahan-kesalahan ini adalah diberi hukuman denda maksimum RM250,000.00 atau hukuman penjara bagi suatu tempoh maksimum tiga (3) tahun atau kedua-duanya sekali dan sebarang kesalahan berikutnya, hukuman denda maksimum atau hukuman penjara bagi suatu tempoh maksimum lima (5) tahun atau kedua-duanya sekali.
Akta Tandatangan Digital 1997	Ringkasan: Akta untuk mengawal perakuan yang sah pada dokumen elektronik dan mengiktiraf kesahan tandatangan digital. Akta ini mengesahkan bahawa di mana terdapat perundangan yang memerlukan kepada tandatangan atau juga menyatakan akibat ketiadaan tandatangan, maka adalah memadai dengan menyediakan tandatangan digital. Apa yang dapat disimpulkan daripada peruntukan ini ialah kesan mana-mana dokumen yang mengandungi tandatangan digital adalah sama seperti mana dokumen yang bertandatangan tulisan tangan.

Nama Undang-Undang	Ringkasan Undang-Undang/URL
Akta Suruhanjaya Komunikasi dan Multimedia 1998 (Akta 589)	Pindaan: *Malaysia Communications and Multimedia Commission (Amendment) Act 2002 (Act A1148)* *Malaysian Communications and Multimedia Commission (Amendment) Act 2002 (Act 1231)* Ringkasan: Akta untuk mengadakan peruntukan bagi penubuhan Suruhanjaya Komunikasi dan Multimedia Malaysia yang mempunyai kuasa untuk menyelia dan mengawal aktiviti-aktiviti komunikasi dan multimedia Malaysia, dan menguatkuasakan undang-undang komunikasi dan multimedia Malaysia, dan bagi perkara-perkara yang berkaitan. Akta ini meliputi komponen Suruhanjaya, kuasa dan fungsi Suruhanjaya, kakitangan Suruhanjaya, Kumpulan Wang Suruhanjaya serta maklumat am Suruhanjaya.
Akta Jenayah Komputer 1997	Ringkasan: Akta untuk mengadakan peruntukan bagi kesalahan berhubung dengan penyalahgunaan komputer.
Akta Hakcipta (Pindaan) 1997	Ringkasan: Antara sebab utama pindaan ini ialah berikutan masalah pemindahan karya hakcipta melalui internet. Akta Hakcipta (Pindaan) 1997, mengakui tiga (3) bentuk baru pelanggaran hakcipta di bawah Seksyen 41 Akta Hakcipta 1987. Kesalahan tersebut adalah: (a) Merosakkan atau menyebabkan kerosakan sebarang tindakan kesan teknologi yang digunakan oleh pencipta berkaitan dengan mempergunakan haknya dan pelanggaran akta tidak dibenarkan;

PENDAHULUAN

Buku panduan ini menjelaskan peranan ICTSO Jabatan/Agensi Negeri yang perlu dilaksanakan dan beberapa perkara yang perlu difahami oleh CIO. Buku panduan ini dikeluarkan bagi membantu ICTSO memahami peranan dan tanggungjawabnya bagi melaksanakan program, penguatkuasaan dan pemantauan keselamatan ICT di Jabatan/Agensi masing-masing.

SYARAT-SYARAT PERLANTIKAN ICTSO

Perkara-perkara yang harus dipertimbangkan bagi tujuan perlantikan ICTSO

i. Sah dalam jawatan;
ii. Tiada rekod tindakan tatatertib/jenayah;
iii. Skim Pegawai Sistem Maklumat (F)- Gred F29 ke atas (jika ada) atau setara atau selain daripada skim F - Gred 44 ke atas (jika ada) atau setara; dan
iv. Mempunyai pengetahuan dalam bidang ICT khususnya dalam keselamatan ICT, pentadbiran sistem, rangkaian dan operasi.

GARIS PANDUAN PERLANTIKAN ICTSO

i. Mendaftar perlantikan ICTSO Jabatan/Agensi Negeri kepada pihak MAMPU dengan menggunakan borang pendaftaran ICTSO MAMPU dan borang perlantikan ICTSO PSUKPP. Perlantikan ICTSO dan sebarang pertukaran perlu dimaklumkan kepada ICTSO PSUKPP dan MAMPU.
ii. Mengemaskini maklumat ICTSO Jabatan/Agensi Negeri di laman MyICTSO Sektor Awam.

Terma Rujukan Tugas ICTSO?

TUGAS 1	Menentukan semua pegawai dan staf jabatan memahami keperluan standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Negeri/Agensi.
TUGAS 2	Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT. Proses penilaian risiko adalah proses menganalisis dan menterjemahkan risiko.
TUGAS 3	Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT.
TUGAS 4	Melaporkan kepada CERT Negeri/CERT Agensi sebarang insiden pelanggaran keselamatan ICT.

Senarai Undang-Undang Berkaitan Siber Malaysia

Nama Undang-Undang	Ringkasan Undang-Undang/URL
Akta Komunikasi dan Multimedia 1998 (Akta 588)	Pindaan: *Communications and Multimedia (Amendment) Act 2004* Ringkasan: Akta ini diwujudkan untuk mengadakan peruntukan dan mengawal selia industri komunikasi dan multimedia yang menjurus ke arah percantuman dan perkara-perkara yang berkaitan dengannya. Akta ini adalah berdasarkan kepada prinsip-prinsip asas bagi ketulusan dan kejelasan *(transparency and clarity)*; pertambahan persaingan dan pengurangan pengawalan (*more competition and less regulation*); *flexibility* dan sebagainya. Akta ini meliputi komponen Kuasa dan Tatacara Menteri, tribunal rayuan, lesen, kuasa dan tatacara Suruhanjaya Komunikasi dan Multimedia Malaysia, Pengawal Seliaan Teknik, perlindungan pengguna, Pengawal Seliaan Sosial, maklumat am serta peruntukan. Objektif akta ini adalah untuk:. (a) menggalakkan matlamat dasar kebangsaan bagi industri komunikasi dan multimedia; (b) mewujudkan rangka kerja perlesenan dan pengawalseliaan bagi menyokong matlamat dasar kebangsaan bagi industri komunikasi dan multimedia; (c) mewujudkan kuasa dan fungsi bagi Suruhanjaya Komunikasi dan Multimedia Malaysia; dan (d) mewujudkan kuasa dan tatacara bagi pentadbiran Akta ini.

Apakah Undang-Undang Siber Yang Diwujudkan?

Tiga (3) Undang-undang Siber telah digubal pada 1997 di bawah peruntukan Akta Hakcipta 1997 iaitu Akta Jenayah Komputer 1997, Akta Tandatangan Digital 1997 dan Akta Teleperubatan 1997 manakala 1998, Akta Komunikasi dan Multimedia 1998 (CMA 1998) dan Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 diluluskan untuk menggantikan Akta Komunikasi 1950 dan Akta Penyiaran 1988.

Bagaimana Undang-Undang Siber Dapat Mengawal Pelaksanaan Program ICT dan Keselamatan Transaksi secara Elektronik ICT?

Dengan adanya Undang-undang Siber ini dapat melindungi industri dari penyalahgunaan atau menjalankan aktiviti-aktiviti yang tidak sah. Selain itu, maklumat juga diberikan dengan jelas berkaitan terma-terma yang perlu diikuti selaras dengan undang-undang.

Undang-Undang yang Diwujudkan Menyatakan Hukuman atau Penalti yang Jelas Kepada Pesalah Siber

Sebagai contoh, negara mempunyai Akta Jenayah Komputer 1997 yang turut menyatakan hukuman tegas kepada pesalah yang mencuri data secara tidak sah atau melalui spam dan sebagainya. Ini secara tidak langsung mengurangkan kadar jenayah siber bagi memastikan sektor teknologi maklumat dan komunikasi (ICT) mampu terus berkembang pesat.

TUGAS 5	Membantu dalam pembangunan khusus bagi standard atau garis panduan yang mematuhi keperluan Rangka Dasar Keselamatan ICT bagi semua aplikasi dalam jabatan.
TUGAS 6	Sentiasa berusaha meningkatkan pengetahuan supaya mengetahui ancaman-ancaman, teknologi dan kaedah-kaedah kawalan maklumat/aset ICT terkini melalui pembacaan, seminar, kursus dan latihan sambil bekerja
TUGAS 7	Sentiasa bersedia dan menyebarkan amaran awal terhadap ancaman-ancaman yang boleh menyebabkan kerosakan besar kepada aset ICT, contohnya serangan virus terbaru atau jangkitan bot net.
TUGAS 8	Mengurus keseluruhan program-program keselamatan ICT dalam jabatan/agensi.

TUGAS 1

Menentukan semua pegawai dan staf jabatan memahami keperluan standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Negeri/Agensi. Ini boleh dilakukan melalui:

- Mengedarkan dokumen Dasar Keselamatan ICT Negeri Pulau Pinang / Dasar Keselamatan ICT Agensi masing-masing;
- Mengaturkan program-program kesedaran mengenai Dasar Keselamatan ICT;
  - Pelbagai kaedah penerangan seperti dialog, taklimat dan lain-lain bagi program penghijrahan minda dan sikap positif terhadap peri pentingnya menjamin keselamatan ICT
  - Mengingatkan pegawai dan staf tentang perlunya memahami Dasar Keselamatan ICT
- Pengukuran tahap kepekaan dan program pemahaman;
- Penyediaan laporan pemahaman bagi memastikan semua peringkat pegawai dan staf telah faham mengenai Dasar Keselamatan ICT; dan
- Pemantauan program pemahaman Dasar Keselamatan ICT

UNDANG-UNDANG SIBER

Latar Belakang

Malaysia telah melalui era pertanian dan era perindustrian dalam usaha membangunkan negara ini dan kini sedang memasuki era teknologi maklumat dan komunikasi (ICT). Dalam ledakan maklumat dan teknologi maklumat, Malaysia tidak ketinggalan sekali gus mendorongnya untuk mewujudkan satu projek yang dikenali sebagai Multimedia Super Corridor (MSC).

Projek ini bertujuan sebagai satu proses peralihan ke era maklumat serta pada masa yang sama memesatkan pertumbuhan industri ICT, telekomunikasi dan multimedia di negara ini. Ke arah kejayaan pelaksanaan aplikasi ini, satu rangka perundangan siber yang komprehensif diperkenalkan untuk menggalakkan pelaburan ICT dan perniagaan dalam industri multimedia dan penggunaan aplikasi multimedia dengan harapan besar agar teknologi canggih, para teknokarat dan sumber manusia mahir atau intelektual dari negara-negara maju dapat dibawa ke Malaysia untuk membantu meletakkan Malaysia dalam arus global penempatan yang berteraskan *competitive advantage* dan kompetensi teras ke arah kecapaian misi Wawasan 2020.

(b) Keperluan-keperluan keselamatan teknologi maklumat dan komunikasi (ICT)

(i) Kriteria tandatangan digital dan cop mohor elektronik yang bersesuaian dengan tujuan kegunaannya;

(ii) Langkah-langkah keselamatan terhadap akses tanpa izin, pengubahsuaian tanpa izin, penghalang perkhidmatan dan penyangkalan; dan

(iii) Prosedur pemulihan bencana.

(c) Pengurusan rekod elektronik

(i) Pengurusan dan Penyelenggaraan dokumen elektronik.

Dokumen Rujukan

Rujukan dokumen Arahan Teknologi Maklumat, sila lawati URL di bawah :

http://www.mampu.gov.my/mampu/pdf/arahan_it_bm.pdf

TUGAS 2

Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT. Proses penilaian risiko adalah proses menganalisis dan menterjemahkan risiko. Proses penilaian ini boleh dilakukan melalui aktiviti-aktiviti berikut:

- Menentukan skop dan metodologi penilaian. Penilaian risiko boleh dilakukan kepada pelbagai kawasan/bidang seperti;
  - Kawasan yang terdedah kepada ancaman pencerobohan.
  - Bahagian infrastruktur ICT yang mudah dicerobohi serta dianggap berisiko tinggi serta kritikal kepada organisasi tersebut.
  - Mengambilkira keselamatan teknikal dan operasional ke dalam rekabentuk sesuatu aplikasi yang baru.
  - Saluran telekomunikasi.
  - Pusat Data.
  - Keseluruhan organisasi.
- Metodologi boleh dilakukan secara formal atau tidak formal, terperinci atau ringkas, paras tinggi atau rendah, kuantitatif berasaskan pengiraan, kualitatif berasaskan skala markah, atau gabungan antara metodologi.
- Mengumpul dan menganalisa data. Risiko mempunyai banyak komponen iaitu aset, ancaman, keselamatan, impak dan *likelihood*. Data yang berkaitan dengan kawasan-kawasan dalaman organisasi yang berisiko tinggi perlu dikumpul. Ini boleh dilaksanakan dengan membuat penilaian kualitatif terhadap aset, ancaman, kelemahan, keselamatan, impak dan *likelihood.*

- Menterjemah keputusan analisa risiko. Keputusan analisa risiko ialah alat yang paling berkesan dan amat membantu pengurusan atasan dalam pemilihan langkah-langkah keselamatan yang paling efektif. Untuk mencapai hasrat ini keputusan dari analisa risiko yang diterjemahkan itu mestilah risiko yang paling kritikal. Ini dapat membantu pengurusan untuk memberi keutamaan kepada bahagian dalam infrastruktur ICT yang perlu diberi perlindungan.

TUGAS 3

Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT. Pelan Rancangan Pematuhan ini mengandungi aktiviti-aktiviti berikut:

- Menyediakan senarai semak pematuhan keselamatan ICT berdasarkan infrastruktur setempat;
- Menggalakkan amalan *'best practice'* dalam aspek keselamatan ICT (seperti yang tercatat dalam senarai semak);
- Mengukur tahap pematuhan di kalangan pegawai dan staf jabatan/agensi;
- Menyediakan laporan pematuhan merangkumi kelemahan yang dikenalpasti serta cadangan langkah-langkah pembetulan;
- Memantau langkah-langkah yang dicadangkan dalam laporan tersebut;
- Mengambil tindakan tertentu lanjutan berlakunya sebarang pelanggaran;
  - Penyemakan semula Pelan Perancangan Pematuhan Keselamatan ICT dengan Dasar Keselamatan ICT;
  - Melaporkan insiden pelanggaran

Arahan Teknologi Maklumat

Apa itu Arahan Teknologi Maklumat?

Arahan Teknologi Maklumat (*IT instructions*) adalah satu garis panduan bertujuan menyokong Akta Aktiviti Kerajaan Elektronik 2007 (EGAA 2007) dalam memudahkan cara transaksi elektronik.

Garis panduan ini adalah keperluan minima untuk semua agensi Kerajaan Persekutuan yang telah bersedia atau dalam proses persediaan melaksanakan transaksi elektronik.

Mengapa Arahan Teknologi Maklumat Diadakan?

Garis Panduan ini adalah penting bagi sesebuah organisasi Kerajaan Persekutuan bagi memastikan kejayaan pelaksanaan projek ICT dari segi penyeragaman pengoperasian transaksi elektronik.

Bidang-bidang Utama Arahan Teknologi Maklumat serta Skopnya

(a) Sistem Aplikasi

(i) Peraturan capaian bagi perkhidmatan Kerajaan Elektronik dan borang elektronik;

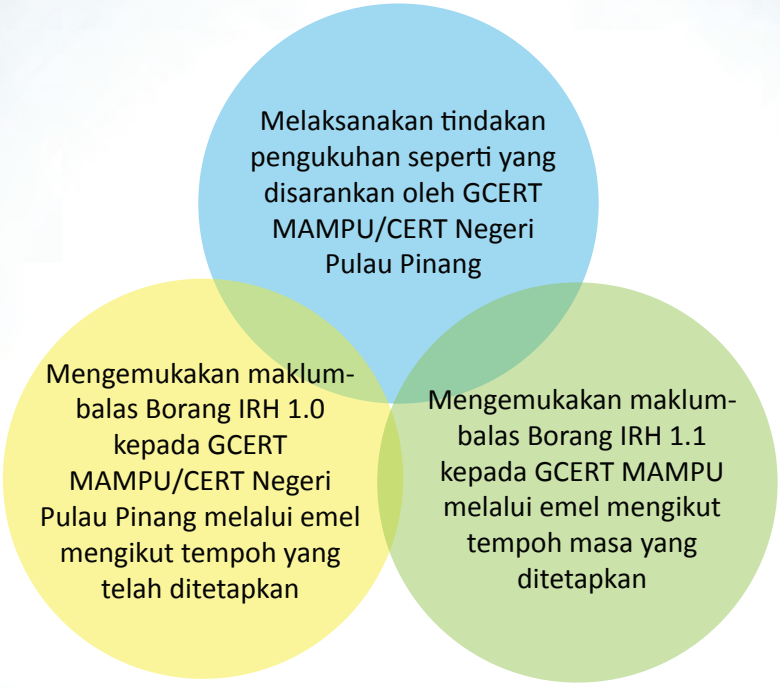
(ii) Standard teknologi maklumat;

(iii) Prosedur berkaitan kemasukan data, semakan dan pengesahan mesej;

(iv) Garis panduan untuk pembayaran dan penerimaan wang; dan

(v) Merekodkan masa, akaun penerimaan dokumen-dokumen elektronik atau mesej-mesej.

Peranan ICTSO



Borang yang digunapakai

(a) PTMKN-04-01 : Borang IRH 1.0 MAMPU

(b) PTMKN-04-02 : Borang IRH 1.1 MAMPU

(c) PTMKN-04-03 : Senarai Semak Siasatan Awal CERT NEGERI

(d) PTMKN-04-04 : Borang IRH 1.0 CERT NEGERI

(e) PTMKN-04-05 : Laporan Imbasan Hos CERT NEGERI

(f) PTMKN-04-06 : Borang IRH 1.1 CERT NEGERI

- Membuat audit terhadap bahagian-bahagian infrastruktur ICT setempat yang berisiko tinggi berdasarkan senarai semak pematuhan tersebut;
- Menyediakan laporan audit;
- Menterjemah laporan tersebut dengan memberikan cadangan-cadangan pembaikan;
- Berdasarkan dari laporan audit, jika keputusan laporan menunjukkan ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT maka tindakan pematuhan perlu dinasihatkan dari segi:
  - Status persediaan masa kini.
  - Keperluan teknologi untuk pemulihan.
  - Sumber khusus untuk pemulihan.
  - Sokongan kritikal sistem maklumat
- Mengadakan sesi *lesson learnt* dalam bentuk senarai cadangan perubahan bagi mendapatkan persetujuan dari pengurusan atasan serta melaksanakannya setelah persetujuan diterima.

TUGAS 4

Melaporkan kepada CERT Negeri/CERT Agensi sebarang insiden pelanggaran keselamatan ICT.

- Melaporkan kejadian insiden kepada CERT Negeri/CERT Agensi dan CIO Jabatan/Agensi masing-masing.
- Mengisi Borang IRH 1.0 dan mengembalikan kepada kumpulan CERT ikut tempoh yang ditetapkan. Menyerahkan log fail untuk dianalisa oleh kumpulan CERT.
- Melaksanakan tindakan pengukuhan seperti yang disarankan oleh kumpulan CERT.

- Mengisi Borang IRH 1.1 dan mengembalikan kepada kumpulan CERT ikut tempoh yang ditetapkan.
- Memfailkan laporan imbasan hos dam laporan analisa fail log dari kumpulan CERT.

TUGAS 5

Membantu dalam pembangunan khusus bagi standard atau garis panduan yang mematuhi keperluan Rangka Dasar Keselamatan ICT bagi semua aplikasi dalam jabatan.

- Memberi khidmat nasihat dan tunjuk ajar bagi membangunkan standard dan garis panduan yang menepati keperluan keselamatan bagi sistem aplikasi jabatan.
- Menyemak standard dan garis panduan sistem operasi aplikasi sedia ada dan memberi cadangan pembaikan.

TUGAS 6

Sentiasa berusaha meningkatkan pengetahuan supaya mengetahui ancaman-ancaman, teknologi dan kaedah-kaedah kawalan maklumat/aset ICT terkini melalui pembacaan, seminar, kursus dan latihan sambil bekerja

- *Self study*.
- Menghadiri seminar yang bersesuaian.
- Mengadakan rangkaian workgroup dalam keselamatan ICT sama ada dengan pakar tempatan atau luar negara.

Prosedur Pengendalian Insiden Keselamatan ICT

Apa itu insiden keselamatan ICT?

Insiden keselamatan ICT merupakan musibah *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

Persijilan MS ISO 9001:2008

Prosedur pengendalian insiden keselamatan ICT yang diuruskan oleh PSUKPP telah mendapat persijilan MS ISO 9001 pada tahun 22 Ogos 2011.

Tujuan dipersijilkan

Untuk memastikan insiden keselamatan ICT dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden.

Pengendalian Insiden Keselamatan ICT daripada GCERT MAMPU

Pengendalian Insiden Keselamatan ICT daripada PRISMA

Pengendalian Insiden Keselamatan ICT CERT Negeri Pulau Pinang

Peranan Jabatan/Agensi di dalam melaksanakan EGAA

Jabatan/Agensi yang ingin melaksanakan EGAA perlulah mengenalpasti aktiviti-aktiviti yang hendak dilaksanakan secara elektronik dan mendapat nasihat daripada Penasihat Undang-Undang Kementerian/ Agensi dan MAMPU. Jabatan/Agensi hendaklah menyediakan aplikasi secara elektronik dan memastikan keberkesanan aplikasi tersebut seperti yang ditetapkan di dalam Arahan Teknologi Maklumat sebelum EGAA dikuatkuasakan.

Dimanakah agensi boleh mendapat bantuan khidmat nasihat mengenai EGAA?

Jabatan/Agensi boleh mendapatkan nasihat daripada MAMPU (Jabatan Perdana Menteri), Jabatan Peguam Negara dan Penasihat Undang-Undang Kementerian.

Dokumen-dokumen Rujukan

(a) Akta Aktiviti Kerajaan Elektronik, Akta 680
(b) Arahan Teknologi Maklumat

Rujukan dokumen Akta Aktiviti Kerajaan Elektronik, sila lawati URL di bawah :

http://www.mampu.gov.my/perkhidmatan/egaa

TUGAS 7

Sentiasa bersedia dan menyebarkan amaran awal terhadap ancaman-ancaman yang boleh menyebabkan kerosakan besar kepada aset ICT, contohnya serangan virus terbaru atau jangkitan bot net.

- *Self study*.
- Menghadiri seminar yang bersesuaian.
- Mengadakan rangkaian workgroup dalam keselamatan ICT sama ada dengan pakar tempatan atau luar negara.

TUGAS 8

Mengurus keseluruhan program-program keselamatan ICT dalam jabatan/agensi.

- Memantau dan menguruskan program-program keselamatan ICT.
- Membuat hebahan keselamatan ICT secara berkala menggunakan mana-mana platform yang bersesuaian.

Direktori ICTSO

Direktori ICTSO untuk Jabatan/Agensi boleh dirujuk melalui URL seperti di bawah:

http://intra.penang.gov.my/ictso.php

CERT Negeri Pulau Pinang

Bila CERT Negeri Pulau Pinang Ditubuhkan?

Jawatankuasa *Computer Emergency Response Team* (CERT) Negeri Pulau Pinang ditubuhkan pada 17 April 2008.

Peranan CERT Negeri Pulau Pinang

(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;
(b) Merekod dan menjalankan siasatan awal insiden yang diterima.
(c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baikpulih minima;
(d) Menghubungi dan melapor insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya;
(e) Menasihat agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan;
(f) Menyebarkan makluman berkaitan kepada agensi di bawah kawalannya;
(g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

AKTA AKTIVITI KERAJAAN ELEKTRONIK (EGAA)

Apa itu Akta Aktiviti Kerajaan Elektronik atau *Electronic Government Activity* (EGAA)? (Akta 680)

EGAA adalah suatu Akta untuk mengadakan peruntukan bagi pengiktirafan undang-undang mesej elektronik dalam urusan antara Kerajaan dengan orang awam, penggunaan mesej elektronik untuk memenuhi kehendak undang-undang dan untuk membolehkan serta memudahkan urusan melalui penggunaan cara elektronik dan perkara-perkara lain yang berkaitan dengannya.

Bila EGAA berkuatkuasa?

EGAA telah berkuatkuasa pada 1 Januari 2008.

Tujuan EGAA diwujudkan

EGAA diwujudkan bagi membolehkan Kementerian/Agensi Kerajaan melaksanakan sesuatu aktiviti di dalam sesuatu Akta secara elektronik.

Pemakaian EGAA

EGAA hanya terpakai bagi Undang-undang Persekutuan yang ditetapkan mengikut Seksyen 6 di dalam Akta tersebut.

(i) Bidang 09: Pengurusan Pengendalian Insiden Keselamatan

(j) Bidang 10: Pengurusan Kesinambungan Perkhidmatan

(k) Bidang 11: Pematuhan

Dokumen-dokumen Rujukan

Antara pekeliling-pekeliling dan Surat Arahan yang berkaitan ialah :

Surat Pekeliling Setiausaha Kerajaan Bil 1 Tahun 2009

Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi dan Komunikasi Kerajaan

Malaysia Public Sector Management of Information and Communication Technology Security Handbook (MyMIS) 2002

Pekelilling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)

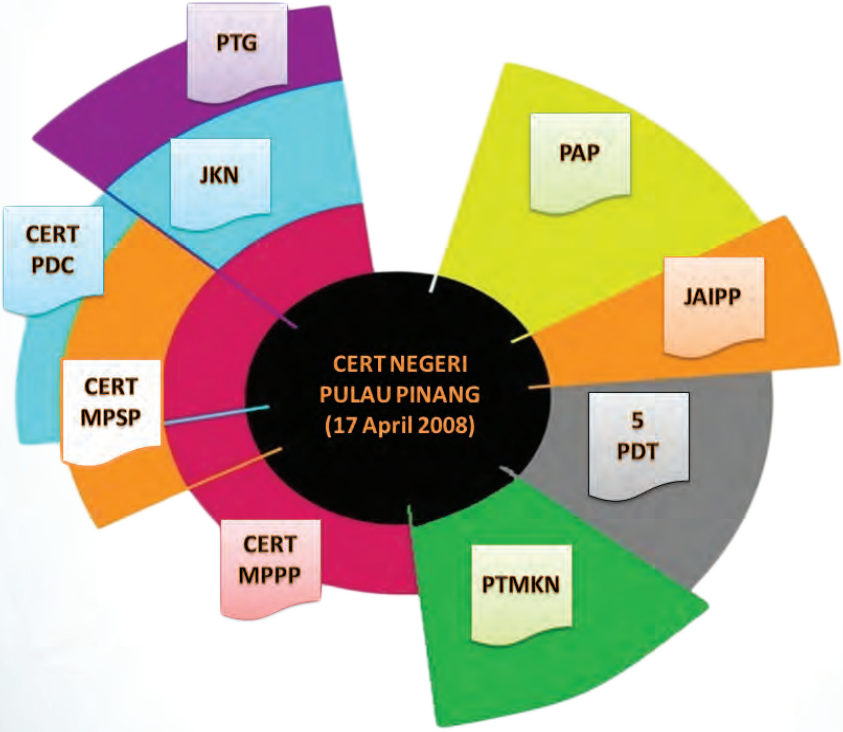
Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan

Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam

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

Surat Arahan Ketua Setiausaha Negara - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar *(Wireless Local Area Network)* di Agensi-Agensi Kerajaan (20 Oktober 2006)

Struktur CERT Negeri Pulau Pinang



Dasar Keselamatan ICT Negeri

Apa itu Dasar Keselamatan ICT?

Dasar Keselamatan ICT adalah merupakan peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aser ICT Kerajaan Negeri Pulau Pinang.

Kepentingan Dasar Keselamatan ICT dalam Pelaksanaan Program ICT Sektor Awam

Dasar Keselamatan ICT adalah dokumen penting dan amat diperlukan bagi menjamin kesinambungan segala urusan agensi dalam melaksanakan program ICT Sektor Awam dengan meminimumkan kesan insiden keselamatan ICT.

Skop Dasar Keselamatan ICT

Dasar Keselamatan ICT meliputi semua sumber atau aset ICT yang digunakan seperti :

(a) Maklumat (contoh : fail, dokumen, data elektronik)

(b) Perisian (contoh : aplikasi dan sistem perisian)

(c) Fizikal (contoh : pusat data, komputer, peralatan komunikasi dan media magnet)

Prinsip-prinsip Dasar Keselamatan ICT

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT yang perlu difahami adalah seperti :

- Akses atas dasar perlu mengetahui
- Hak akses minimum
- Akauntabiliti
- Pengasingan
- Pengauditan
- Pematuhan
- Pemulihan
- Saling Bergantungan

Penggubalan Dasar Keselamatan ICT Negeri

Perkara-perkara berikut telah diambil kira semasa penggubalan Dasar Keselamatan ICT:

(a) Bidang 01: Pembangunan dan Penyelengaraan Dasar

(b) Bidang 02: Organisasi Keselamatan

(c) Bidang 03: Pengurusan Aset

(d) Bidang 04: Keselamatan Sumber Manusia

(e) Bidang 05: Keselamatan Fizikal dan Persekitaran

(f) Bidang 06: Pengurusan Operasi dan Komunikasi

(g) Bidang 07: Kawalan Operasi

(h) Bidang 08: Perolehan, Pembangunan dan Penyelengaraan Sistem