



KERAJAAN NEGERI JOHOR

DASAR KESELAMATAN

TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

(ICT)

Disediakan oleh:
UNIT SAINS TEKNOLOGI DAN ICT NEGERI JOHOR

VERSI 1.0 | SEPTEMBER 2009

KANDUNGAN

PERKARA	MUKA SURAT
<i>Pendahuluan</i>	
1.1 Pengenalan	1
1.2 Objektif Dasar Keselamatan ICT Kerajaan Negeri Johor	1
1.3 Skop Dasar Keselamatan ICT Kerajaan Negeri Johor	2
<i>Penyataan Dasar Keselamatan ICT</i>	5
2.1 Prinsip-prinsip Dasar Keselamatan ICT Kerajaan Negeri Johor	6
2.2 Pindaan Dan Kemas kini	11
2.3 Maklumat Lanjut	12
<i>Tafsiran</i>	13
<i>Pelaksanaan Dasar Keselamatan ICT</i>	
4.0 Pelaksanaan Dasar Keselamatan ICT Kerajaan Negeri Johor	15
4.1 Pemakaian Dasar Keselamatan ICT Kerajaan Negeri Johor	15
4.2 Semakan dan Pindaan Dasar	16
4.3 Tanggungjawab Kerajaan Negeri Johor	16
<i>Pengurusan Keselamatan ICT</i>	
5.0 Pengurusan Keselamatan ICT Kerajaan Negeri Johor	17
5.1 Struktur Organisasi	17
5.2 Pihak Luar/Asing	18
5.3 Jawatankuasa Pengurusan Keselamatan ICT Kerajaan Negeri Johor	19
<i>Pengurusan Aset</i>	
6.0 Pengurusan Aset	24
6.1 Tanggungjawab Ke Atas Aset	24
6.2 Pengelasan Maklumat	24
6.3 Pelabelan dan Pengendalian Maklumat	25

Keselamatan Sumber Manusia

7.0	Keselamatan Sumber Manusia	26
7.1	Sebelum Berkhidmat	26
7.2	Dalam Perkhidmatan	27
7.3	Bertukar Atau Tamat Perkhidmatan	28

Keselamatan Fizikal dan Persekitaran

8.0	Keselamatan Fizikal dan Persekitaran	29
8.1	Kawalan Kawasan Terhad	29
8.2	Keselamatan Peralatan	30
8.3	Prasarana Sokongan	32
8.4	Penyelenggaraan Peralatan	34
8.5	Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	34
8.6	Pengendalian Peralatan Luar Yang Dibawa Masuk / Keluar	35
8.7	Pelupusan dan Kitar Semula Peralatan	35
8.8	<i>Clear Desk</i> dan <i>Clear Screen</i>	36

Pengurusan Operasi Dan Komunikasi

9.0	Pengurusan Operasi Dan Komunikasi	37
9.1	Tanggungjawab Dan Prosedur Operasi	37
9.2	Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain	38
9.3	Perancangan Dan Penerimaan Sistem	38
9.4	Perlindungan Dari <i>Malicious</i> dan <i>Mobile Code</i>	39
9.5	<i>Backup</i> dan <i>Restore</i>	39
9.6	Pengurusan Keselamatan Rangkaian	40
9.7	Pengendalian Peralatan Penyimpanan Maklumat	40
9.8	Pertukaran Maklumat	41
9.9	Perkhidmatan e-Dagang (<i>e-Commerce</i>)	41
9.10	Pemantauan	42

Kawalan Capaian

10.0	Pengurusan Kawalan Capaian	44
10.1	Keperluan Kawalan Capaian	44

10.2	Pengurusan Capaian Pengguna	45
10.3	Tanggungjawab Pengguna	46
10.4	Kawalan Capaian Rangkaian	46
10.5	Kawalan Capaian Sistem Pengoperasian	47
10.6	Kawalan Capaian Aplikasi Dan Maklumat	48
10.7	Peralatan Mudah Alih Dan Kerja Jarak Jauh	49

Perolehan, Pembangunan Dan Penyenggaraan Sistem Maklumat

11.0	Perolehan, Pembangunan dan Penyenggaraan Sistem Maklumat	50
11.1	Keperluan Keselamatan Sistem Maklumat	51
11.2	Pemprosesan Aplikasi Dengan Tepat	51
11.3	Kawalan Kriptografi	52
11.4	Keselamatan Fail-fail Sistem	52
11.5	Keselamatan Dalam Proses Pembangunan Dan Sokongan	52
11.6	Pengurusan Teknikal Kerentanan (Vulnerability)	53

Pengurusan Pengendalian Insiden Keselamatan

12.0	Pengurusan Pengendalian Insiden Keselamatan	54
12.1	Insiden Keselamatan	54
12.2	Melapor Kejadian Insiden	55
12.3	Menentukan Keutamaan Tindakan Ke Atas Insiden	55
12.4	Mengendalikan Insiden Kritikal	56

Pengurusan Kesenambungan Perkhidmatan

13.0	Kesenambungan Perkhidmatan	57
13.1	Tanggungjawab Melaksanakan Penilaian Risiko Keselamatan ICT	57
13.2	Skop Penilaian Risiko Keselamatan ICT	57
13.3	Penentuan Tindakan Untuk Mengendalikan Risiko Keselamatan ICT	58
13.4	Pelan Kesenambungan Perkhidmatan	58

Pematuhan

14.0	Pematuhan Keperluan Perundangan	60
14.1	Pematuhan Dasar	60
14.2	Keperluan Perundangan	60
14.3	Pelanggaran Perundangan	65

PENDAHULUAN

1.1 Pengenalan

Kerajaan Negeri Johor bertanggungjawab untuk memastikan keselamatan aset teknologi maklumat dan komunikasi (*information and communication technology*), ringkasnya ICT, yang dimiliki atau di bawah jagaan dan kawalannya. Ini termasuk semua data, peralatan, rangkaian dan kemudahan ICT. Tanggung jawab ini juga harus dipikul oleh semua yang menggunakan aset ICT Kerajaan Negeri Johor.

1.2 Objektif Dasar Keselamatan ICT Kerajaan Negeri Johor

Dasar Keselamatan ICT Kerajaan Negeri Johor diwujudkan untuk menjamin kesinambungan urusan Kerajaan Negeri dengan meminimumkan kesan insiden keselamatan ICT. Ciri-ciri utama keselamatannya adalah kerahsiaan, integriti dan kebolehsediaan.

Objektif utama Dasar Keselamatan ICT Kerajaan Negeri Johor adalah seperti berikut:

- (a) Memastikan kelancaran operasi Kerajaan Negeri Johor dan meminimumkan kerosakan atau kemusnahan;
- (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
- (c) Mencegah salah guna atau kecurian aset ICT. Dasar Keselamatan ICT Kerajaan Negeri Johor ini juga bertujuan memudahkan perkongsian maklumat sesuai dengan keperluan operasi. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

1.3 Skop Dasar Keselamatan ICT Kerajaan Negeri Johor

- 1.3.1 Sistem ICT Kerajaan Negeri Johor terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. Sistem ini adalah aset yang amat berharga di mana masyarakat, pihak swasta dan juga Kerajaan Negeri bergantung untuk menjalankan urusan rasmi dengan lancar. Oleh itu, Dasar Keselamatan ICT Kerajaan Negeri Johor menetapkan keperluankeperluan asas berikut:
- (a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
 - (b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan Kerajaan Negeri, perkhidmatan dan masyarakat.
- 1.3.2 Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantung antara satu dengan lain kerap kali mewujudkan pelbagai kelemahan. Seseengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenal pasti dan ditangani sewajarnya.
- 1.3.3 Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT Kerajaan Negeri Johor merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

- (a) Data dan Maklumat – Dokumen, salinan maklumat dan *intellectual document* di mana ia digunakan untuk mencapai misi dan/atau objektif organisasi. Contoh: dokumentasi sistem, prosedur operasi, rekod-rekod perniagaan, profil pelanggan dan lain-lain lagi.

- (b) Peralatan ICT - Aset fizikal yang boleh disentuh yang mana ia digunakan untuk menyokong maklumat, memproses, dan kemudahan storan kepada organisasi. Contoh: komputer, pelayan, peralatan komputer, media storan dan lain-lain lagi.

- (c) Komunikasi dan Peralatan Rangkaian – Perkhidmatan atau sistem (tidak dalam keadaan *standalone* perkakasan fizikal atau perisian) yang menyokong lain-lain aset untuk melaksanakan fungsi masing-masing. Contoh:
 - i. Perkhidmatan capaian:
 - 1. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
 - 2. Sistem Capaian Terhad seperti sistem kad akses
 - ii. Perkhidmatan sokongan: utiliti seperti elektrik, penghawa dingin dan sistem penggera api.

- (d) Perisian - Perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau perisian pejabat yang menyediakan maklumat – kemudahan proses kepada organisasi.
Contoh : aplikasi-aplikasi, peralatan pembangunan, utiliti, perisian sistem, dan lain-lain lagi.

- (e) Manusia - Individu yang mempunyai pengetahuan dan kemahiran untuk mengendalikan fungsi harian skop agensi dalam mencapai objektif atau misi.

(f) Premis Komputer dan Komunikasi - Semua kemudahan serta premis yang diguna untuk menempatkan perkara (a)-(d) di atas.

1.3.4 Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

1.3.5 Di samping itu, Dasar Keselamatan ICT Kerajaan Negeri Johor ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

PERNYATAAN DASAR KESELAMATAN ICT

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala bagi menjamin keselamatan. Keselamatan ICT adalah bermaksud keadaan bagi urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan lancar tanpa gangguan yang boleh menjejaskan keselamatan termasuklah perlindungan kepada aset ICT.

Dasar Keselamatan ICT Kerajaan Negeri Johor merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- (a) Kerahsiaan — Maklumat tidak boleh didedahkan sewenang - wenangnya atau dibiarkan diakses tanpa kebenaran;
- (b) Integriti — Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan; dan
- (c) Kebolehsediaan — Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

2.1 Prinsip-Prinsip Dasar Keselamatan ICT Kerajaan Negeri Johor

Prinsip-prinsip asas kepada Dasar Keselamatan ICT Kerajaan Negeri Johor adalah seperti berikut:

- (a) Akses atas dasar "perlu tahu";
- (b) Hak akses minimum;
- (c) Akauntabiliti;
- (d) Pengasingan;
- (e) Pengauditan;
- (f) Pematuhan;
- (g) Pemulihan; dan
- (h) Saling bergantung.

2.1.1 Akses Atas Dasar Perlu Tahu

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu tahu" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

(a) Klasifikasi Maklumat

Keselamatan ICT Kerajaan Negeri Johor hendaklah mematuhi "Arahan Keselamatan", di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, di manipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan

(b) Tapisan Keselamatan Pengguna

Dasar Keselamatan ICT Kerajaan Negeri Johor adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

2.1.2 Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

2.1.3 Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- (b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- (c) Menentukan maklumat sedia untuk digunakan;
- (d) Menjaga kerahsiaan kata laluan;

- (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penerimaan, penyampaian, pertukaran dan pemusnahan; dan
- (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

2.1.4 Pengasingan

- (a) Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan; dan
- (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- (a) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
- (b) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan
- (c) Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

2.1.5 Pengauditan

- (a) Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta-merta;

- (b) Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer; dan

- (c) Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:
 - i. Mengesan pematuhan atau pelanggaran keselamatan;

 - ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan

 - iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

2.1.6 Pematuhan

Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran Dasar. Pematuhan kepada Dasar Keselamatan ICT Kerajaan Negeri Johor boleh dicapai melalui tindakan berikut:

- (a) Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
- (b) Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;
- (c) Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
- (d) Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

2.1.7 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

- (a) Merumuskan dan menguji Pelan Pemulihan Bencana— (*Disaster Recovery Plan*); dan
- (b) Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk*.

2.1.8 Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:

- (a) Sambungan kepada internet - Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui rangkaian pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui peralatan rangkaian yang dikawal secara terpusat. Dengan itu, penggunaan peralatan rangkaian tidak berpusat tidak dibenarkan;
- (b) *Backbone* Rangkaian - *Backbone* rangkaian akan hanya mengendalikan trafik yang telah di kod untuk meminimumkan intipan;
- (c) Rangkaian Kerajaan Negeri - Semua rangkaian Kerajaan Negeri akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian Kerajaan Negeri dengan rangkaian di peringkat yang seterusnya atau pusat data; dan
- (d) *Server* Kerajaan Negeri - Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di *server* Kerajaan Negeri atau di *server* yang diurus secara pusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitive akan dikodkan.

2.2 Pindaan dan Kemas kini

Dasar Keselamatan ICT Kerajaan Negeri Johor adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi,

prosedur, perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah keselamatan ICT Kerajaan Negeri Johor yang akan dikeluarkan dari semasa ke semasa.

2.3 Maklumat Lanjut

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh ditujukan kepada:

Unit Sains Teknologi Dan ICT Negeri Johor,
Aras 2, Kompleks Menteri Besar,
Pusat Pentadbiran Kerajaan Negeri Johor,
79 100, Nusajaya, Johor Darul Takzim.

Telefon : 07 266 6660 / 6661
Faks : 07 266 1667 / 1668
E-Mel : ustict@johor.gov.my

Dasar Keselamatan ICT Kerajaan ini juga boleh diakses di Laman Web Rasmi Unit Sains Teknologi Negeri Johor : www.johor.gov.my/ustj

TAFSIRAN

- (a) **Risiko**
Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
- (b) **Penilaian Risiko**
Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
- (c) **Ancaman**
Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
- (d) **Kerentanan (*Vulnerability*)**
Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
- (e) **Insiden Keselamatan**
Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat.
- (f) **Aset ICT**
Bermaksud semua yang mempunyai nilai kepada agensi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
- (g) **Penyulitan (*Encryption*)**
Bermaksud menukarkan teks biasa (*plaintext*) kepada bentuk teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses penyahsulitan (*decryption*) digunakan.
- (h) **Clear Desk**
Bermaksud tidak mendedahkan sebarang maklumat yang sensitif di tempat kerja.

- (i) ***Clear Screen***
Bermaksud tidak memaparkan sebarang maklumat sensitif di atas skrin atau yang seumpama dengannya tanpa pengawasan.

- (j) ***Mobile Code***
Bermaksud kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

- (k) **Kriptografi (*Cryptography*)**
Bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

- (l) ***Business Resumption Plan (BRP)***
Bermaksud pelan yang berupaya untuk meneruskan operasi jika berlaku gangguan perkhidmatan. Dalam situasi pelan sukar dilaksanakan sepenuhnya, maka pelan ini seboleh-bolehnya dapat melaksanakan fungsi-fungsi bagi operasi teras.

PELAKSANAAN DASAR KESELAMATAN ICT

Pernyataan Dasar

Kerajaan Negeri Johor hendaklah mewujudkan dan melaksanakan dasar-dasar yang jelas yang dapat menjamin perlindungan ke atas kerahsiaan, integriti dan kebolehsediaan maklumat dan seterusnya menjamin kesinambungan urusan dan perkhidmatan dengan meminimumkan kesan insiden keselamatan.

Objektif

Untuk memberi hala tuju dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

4.0 Pelaksanaan Dasar Keselamatan ICT Kerajaan Negeri Johor

Seksyen ini bertujuan memastikan hala tuju pengurusan Kerajaan Negeri Johor untuk melindungi aset ICT selaras dengan keperluan perundangan. Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri ke atas pelaksanaan dasar dengan dibantu oleh jawatankuasa pengurusan keselamatan ICT yang terdiri dari Ketua Pegawai Maklumat (CIO), Pengarah Unit Sains Teknologi Dan ICT Negeri Johor, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik. Dasar Keselamatan ICT hendaklah diterima pakai oleh pengurusan dan disebarkan kepada setiap warga agensi.

4.1 Pemakaian Dasar Keselamatan ICT Kerajaan Negeri Johor

Dasar Keselamatan ICT Kerajaan Negeri Johor adalah terpakai kepada semua pengguna aset ICT termasuk pembekal dan pakar runding yang berurusan dengan Kerajaan Negeri Johor dan tiada pengecualian diberikan.

4.2 Semakan dan Pindaan Dasar

Dasar Keselamatan ICT Kerajaan Negeri Johor adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT Kerajaan Negeri Johor adalah termasuk yang berikut:

- (a) Menyemak dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan;
- (b) Mengemukakan cadangan perubahan secara bertulis kepada JPIC, Kerajaan Negeri Johor; dan
- (c) Memaklumkan perubahan dasar yang telah dipersetujui kepada semua pengguna.

4.3 Tanggungjawab Kerajaan Negeri Johor

Tanggungjawab Kerajaan Negeri Johor adalah seperti berikut:

- (a) Memberi pendedahan dan penjelasan mengenai Dasar Keselamatan ICT Kerajaan Negeri Johor;
- (b) Menyediakan perkhidmatan pusat untuk menerima laporan insiden keselamatan ICT;
- (c) Penyebaran maklumat dan pelarasan tindakan pembetulan; dan
- (d) Memantau pelaksanaan dan menguatkuasa Dasar Keselamatan ICT Kerajaan Negeri Johor.

PENGURUSAN KESELAMATAN ICT

Pernyataan Dasar

Satu rangka kerja pengurusan keselamatan ICT Kerajaan Negeri Johor perlu diwujudkan supaya keselamatan ICT Kerajaan Negeri Johor dilaksanakan dengan lebih sistematik, lancar dan berkesan.

Objektif

Untuk mengurus keselamatan ICT Kerajaan Negeri Johor.

5.0 Pengurusan Keselamatan ICT Kerajaan Negeri Johor

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri Johor untuk:

- (a) Memastikan semua pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- (b) Mewujud dan mengetuai jawatankuasa pengurusan keselamatan ICT Kerajaan Negeri Johor;
- (c) Memastikan semua keperluan keselamatan ICT (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi; dan
- (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Kerajaan Negeri Johor.

5.1 Struktur Organisasi

Seksyen ini bertujuan untuk memastikan struktur formal diwujudkan untuk mengurus keselamatan ICT Kerajaan Negeri Johor. Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Komitmen pengurusan atasan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus;
- (b) Tanggungjawab yang jelas bagi semua pengguna dalam pengurusan keselamatan ICT;
- (c) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksana dan dikaji secara berkala;
- (d) Memastikan jalinan perhubungan/komunikasi dengan pihak yang terbabit dipelihara; dan
- (e) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.

5.2 Pihak Luar/Asing

Seksyen ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/asing dikawal. Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemrosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;
- (b) Mengenal pasti keperluan keselamatan sebelum member kebenaran capaian atau penggunaan kepada pengguna; dan
- (c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:

- i. Dasar Keselamatan ICT Kerajaan Negeri Johor;

- ii. Tapisan Keselamatan;
- iii. Perakuan Akta Rahsia Rasmi 1972; dan
- iv. Hak Harta Intelek;

5.3 Jawatankuasa Pengurusan Keselamatan ICT Kerajaan Negeri Johor

Seksyen ini bertujuan menerangkan peranan dan tanggungjawab ahli jawatankuasa pengurusan keselamatan ICT Kerajaan Negeri Johor.

(a) Ketua Pegawai Maklumat (CIO)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- ii. Menentukan keperluan keselamatan ICT;
- iii. Membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan

(b) Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- ii. Mengurus keseluruhan program-program keselamatan ICT Kerajaan Negeri Johor;
- iii. Menkuatkuasakan Dasar Keselamatan ICT Kerajaan Negeri Johor;

- iv. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Kerajaan Negeri Johor kepada semua pengguna;
- v. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT Kerajaan Negeri Johor;
- vi. Melaksanakan pengurusan risiko;
- vii. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- viii. Memberi amaran kepada agensi terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti virus dan penggadam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah-langkah perlindungan yang bersesuaian;
- ix. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) Kerajaan Negeri Johor, Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT) MAMPU dan memaklukkannya kepada Setiausaha Kerajaan Negeri, CIO dan Pengurus ICT;
- x. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
- xi. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan Ict Kerajaan Negeri Johor; dan
- xii. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

(c) Pengurus ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- ii. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan Kerajaan Negeri Johor;
- iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan;
- iv. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Kerajaan Negeri Johor dilaksanakan; dan
- v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas.

(d) Pentadbir Sistem ICT dan Pentadbir Rangkaian ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- ii. Menjaga kerahsiaan kata laluan;
- iii. Menjaga kerahsiaan konfigurasi aset ICT;
- iv. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna yang digantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas;

- v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar / asing yang berhenti atau tamat projek;
- vi. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan;
- vii. Memantau aktiviti capaian harian pengguna;
- viii. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran; membatalkan atau memberhentikan dengan serta merta; dan memaklumkan kepada Pengurus ICT untuk tindakan selanjutnya; dan
- ix. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
- x. Menyimpan dan menganalisis rekod jejak audit.

(e) Pengguna Dalaman

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan Negeri Johor;
- ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
- iii. Melaksanakan langkah-langkah perlindungan seperti berikut:
 - ° Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan,

penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;

- Menjaga kerahsiaan kata laluan;
- Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; dan
- Menjaga kerahsiaan langkah-langkah keselamatan ICT daridiketahui umum.

iv. Menghadiri program-program kesedaran mengenai keselamatan ICT.

PENGURUSAN ASET

Pernyataan Dasar

Setiap aset perlu dikenal pasti, dikelaskan, didokumenkan dan diselenggarakan.

Objektif

Untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

6.0 Pengurusan Aset

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri untuk mengurus aset ICT di bawah kawalannya.

6.1 Tanggungjawab Ke Atas Aset

Seksyen ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing mengikut peraturan-peraturan yang telah dikeluarkan oleh Kementerian Kewangan Malaysia.

6.2 Pengkelasan Maklumat

Seksyen ini bertujuan memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan. Maklumat hendaklah dikelaskan berdasarkan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada Kerajaan berdasarkan kepada peraturan-peraturan Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan agensi masing-masing.

6.3 Pelabelan dan Pengendalian Maklumat

Pelabelan dan pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penerimaan, penyampaian, penukaran dan pemusnahan hendaklah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan berdasarkan kepada peraturan-peraturan Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan agensi masing-masing.

KESELAMATAN SUMBER MANUSIA

Pernyataan Dasar:

Semua tanggungjawab dan peranan penjawat awam, pembekal, pakar runding dan pihak-pihak lain hendaklah jelas dan didokumentenkan mengikut keperluan dasar keselamatan ICT agensi.

Objektif:

Untuk memastikan semua pihak yang terlibat termasuk penjawat awam, pembekal, pakar runding dan mana-mana pihak yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT.

7.0 Keselamatan Sumber Manusia

Setiausaha Kerajaan Negeri adalah bertanggungjawab ke atas pihak yang terlibat secara langsung atau tidak langsung dalam pengendalian aset ICT di bawah kawalannya dan memerlukan program pembudayaan atau kesedaran mengenai keselamatan.

7.1 Sebelum Berkhidmat

Seksyen ini bertujuan memastikan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
- (b) Menjalankan tapisan keselamatan untuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan
- (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

7.2 Dalam Perkhidmatan

Seksyen ini bertujuan memastikan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT agensi dan meminimumkan risiko kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Memastikan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Kerajaan Negeri Johor;
- (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada penjawat awam, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan
- (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang

berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan Kerajaan Negeri Johor.

7.3 Bertukar Atau Tamat Perkhidmatan

Seksyen ini bertujuan memastikan pertukaran atau tamat perkhidmatan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diurus dengan teratur.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Memastikan semua aset ICT dikembalikan kepada Kerajaan Negeri Johor mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan
- (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan agensi dan/atau terma perkhidmatan.

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Pernyataan Dasar

Premis dan peralatan memproses maklumat hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.

Objektif

Untuk menghalang capaian yang tidak dibenarkan, kerosakan dan gangguan terhadap persekitaran premis, peralatan dan maklumat.

8.0 Keselamatan Fizikal dan Persekitaran

Adalah menjadi tanggungjawab Ketua Jabatan untuk mengesan, mencegah dan menghalang pencerobohan ke atas kawasan yang menempatkan peralatan, maklumat dan kemudahan pemprosesan maklumat yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis dan maklumat berdasarkan kepada peraturan-peraturan Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan Kerajaan Negeri Johor.

8.1 Kawalan Kawasan Terhad

Seksyen ini bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat Kerajaan Negeri Johor.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

- (b) Melindungi kawasan terhad melalui kawalan keluar masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- (c) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk semua yang bekerja di dalam kawasan terhad; dan
- (d) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

8.2 Keselamatan Peralatan

Seksyen ini adalah bertujuan untuk mengelak dari sebarang kehilangan, kerosakan, kecurian atau kompromi ke atas aset ICT dan gangguan ke atas sistem penyampaian agensi.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

- (a) Perkakasan
 - i. Menempatkan dan mengawal peralatan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan menceroboh oleh pihak yang tidak diberi kebenaran dapat dikurangkan; dan
 - ii. Semua cadangan pengubahsuaian, pembelian, penempatan dan pemindahan peralatan-peralatan ICT hendaklah dirujuk terlebih dahulu kepada CIO dan Pengarah Unit Sains Teknologi Dan ICT Negari Johor.

- (b) Dokumen

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

- i. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
 - ii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen;
 - iii. Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan
 - iv. Menggunakan enkripsi ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.
- (c) Media Storan (Disket, pita magnetik, cakera keras, *CD-ROM*, *optical disk*, *flash disk* dan lain-lain)

Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi Kerajaan.

Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat :

- i. Menyediakan ruang penyimpanan dan bekas-bekas keselamatan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- ii. Menghadkan akses kepada pengguna yang dibenarkan sahaja;
- iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan
- iv. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup/restore*.

8.3 Prasarana Sokongan

(a) Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pihak-pihak yang berkaitan. Perkara yang perlu dipatuhi adalah seperti berikut:

- i. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;
- ii. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegahan kebakaran dan pintu kecemasan;
- iii. Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- iv. Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;
- v. Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT;
- vi. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan
- vii. Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.
- viii. Mematuhi peraturan yang telah ditetapkan oleh pihak-pihak yang berkaitan seperti bomba, JKR dan sebagainya.

(b) Bekalan Kuasa

- i. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;
- ii. Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan
- iii. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

(c) Prosedur Kecemasan

- i. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan Kerajaan Negeri Johor;
- ii. Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Kerajaan Negeri Johor;
- iii. Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan
- iv. Mengadakan latihan kecemasan bencana setahun sekali.

(d) Keselamatan Rangkaian

Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut :

- i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

- ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
- iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
- iv. Membuat pelabelan kabel.

8.4 Penyelenggaraan Peralatan

Perkakasan hendaklah disenggarakan berdasarkan peraturan-peraturan semasa bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut :

- (a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara;
- (b) Memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
- (c) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan
- (d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

8.5 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat

Peralatan yang dipinjam hendaklah mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh Pengurusan ICT Kerajaan Negeri Johor bagi membawa keluar perkakasan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan.

Langkah-langkah perlu diambil termasuklah seperti berikut:

- (a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Pengurusan ICT Kerajaan Negeri Johor bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan;
- (b) Melindungi dan mengawal peralatan sepanjang masa;
- (c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan
- (d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.

8.6 Pengendalian Peralatan Luar Yang Dibawa Masuk / Keluar

Bagi peralatan yang dibawa masuk ke tempat-tempat tertentu (*secured area*) seperti pusat data dan bilik telekomunikasi, langkah keselamatan yang perlu diambil adalah seperti berikut:

- (a) Memastikan peralatan yang di bawa masuk tidak mengancam keselamatan ICT Kerajaan Negeri Johor;
- (b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh agensi bagi membawa masuk/keluar peralatan; dan
- (c) Menyemak peralatan yang dibawa keluar tidak mengandungi maklumat Kerajaan Negeri Johor.

8.7 Pelupusan Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kerajaan. Langkah-langkah hendaklah diambil termasuklah

menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi sebelum dilupuskan.

8.8 *Clear Desk dan Clear Screen*

Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan :

- (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
- (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
- (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

PENGURUSAN OPERASI DAN KOMUNIKASI

Pernyataan Dasar

Prosedur pengurusan operasi dan komunikasi hendaklah didokumenkan, diselenggarakan dan mudah didapati apabila diperlukan

Objektif

Untuk memastikan kemudahan pemprosesan maklumat dan komunikasi adalah berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

9.0 Pengurusan Operasi Dan Komunikasi

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri untuk memastikan kesemua kemudahan pemprosesan maklumat adalah terjamin selamat dan berjalan lancar.

9.1 Tanggungjawab Dan Prosedur Operasi

Seksyen ini bertujuan memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemas kini dan sedia diguna pakai oleh pengguna mengikut keperluan;
- (b) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal;

- (c) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaiian dan penyalahgunaan aset agensi; dan
- (d) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.

9.2 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain

Seksyen ini bertujuan memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain;
- (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
- (c) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

9.3 Perancangan Dan Penerimaan Sistem

Seksyen ini bertujuan untuk mengurangkan risiko kegagalan sistem.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum; dan
- (b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.
- (c) Semua urusan penerimaan dan ujian hendaklah direkodkan dengan jelas dan teratur.

9.4 Perlindungan Dari *Malicious* Dan *Mobile Code*

Seksyen ini bertujuan untuk melindungi integriti maklumat dan perisian dari ancaman *malicious code* seperti *viruses*, *worms*, *trojan horses*, *logic bombs*.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code*; dan
- (b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasiya hendaklah memastikan bahawa ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali.

9.5 *Backup* dan *Restore*

Seksyen ini bertujuan untuk mengekalkan integriti, kesediaan maklumat dan kemudahan pemprosesan maklumat . Semua urusan backup dan restore hendaklah didokumenkan dengan teratur.

Perkara yang mesti dipatuhi termasuk membuat dan menguji secara berkala dalam beberapa salinan maklumat dan perisian berdasarkan prosedur *backup* dan *restore* pada premis berbeza.

9.6 Pengurusan Keselamatan Rangkaian

Seksyen ini bertujuan untuk memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang menggunakan rangkaian, termasuk maklumat yang dipindahkan melaluinya; dan
- (b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.

9.7 Pengendalian Peralatan Penyimpanan Maklumat

Seksyen ini bertujuan untuk memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;
- (b) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;

- (c) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan
- (d) Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan.

9.8 Pertukaran Maklumat

Seksyen ini bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam agensi dan mana-mana pihak terjamin.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
- (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar;
- (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi;
- (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan
- (e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan system maklumat agensi.

9.9 Perkhidmatan e-Dagang (e-Commerce)

Seksyen ini bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;
- (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan
- (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

9.10 Pemantauan

Seksyen ini bertujuan untuk mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan dan memastikan rekod log aktiviti tidak boleh diubahsuai dan dicapai oleh pihak yang tidak dibenarkan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
- (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
- (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
- (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

- (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan
- (f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam agensi atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.

KAWALAN CAPAIAN

Pernyataan Dasar

Capaian ke atas maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem.

Objektif

Untuk mengawal capaian ke atas maklumat.

10.0 Pengurusan Kawalan Capaian

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri untuk memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan-kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan.

10.1 Keperluan Kawalan Capaian

Seksyen ini bertujuan mengawal capaian ke atas maklumat, kemudahan-kemudahan proses maklumat, dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu dipastikan termasuk seperti berikut:

- (a) Kawalan capaian ke atas maklumat dan proses perkhidmatan mengikut keperluan keselamatan dan peranan pengguna;
- (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
- (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan
- (d) Kawalan ke atas kemudahan pemrosesan maklumat.

10.2 Pengurusan Capaian Pengguna

Seksyen ini bertujuan memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.

Perkara-perkara yang perlu dipatuhi adalah termasuk :

- (a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;
- (b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;
- (c) Akaun pengguna yang di wujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; dan
- (d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan Kerajaan Negeri Johor dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab seperti berikut:
 - i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan;

- ii. Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditentukan;
- iii. Pengguna bertukar jawatan, tanggungjawab dan/atau bidang tugas;
- iv. Pengguna yang sedang dalam prosiding dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan
- v. Pengguna bertukar, berpindah, bersara dan/atau tamat perkhidmatan.

Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

10.3 Tanggungjawab Pengguna

Seksyen ini bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut :

- (a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;
- (b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan
- (c) Mematuhi amalan *clear desk policy* dan *clear screen policy*.

10.4 Kawalan Capaian Rangkaian

Seksyen ini bertujuan menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian agensi, rangkaian agensi lain dan rangkaian awam;
- (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan, yang menepati kesesuaian penggunaannya; dan
- (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

10.5 Kawalan Capaian Sistem Pengoperasian

Seksyen ini bertujuan untuk memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

- Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Kerajaan Negeri Johor;
- Mewujudkan *audit trail* ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user*;
- Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem;
- Menyediakan kaedah yang sesuai untuk pengesahan capaian (*authentication*); dan
- Menghadkan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Mengawal capaian ke atas sistem operasi menggunakan prosedur *log-on* yang terjamin;

- (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna.
- (c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;
- (d) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi;
- (e) Menamatkan sesebuah sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan;
- (f) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

10.6 Kawalan Capaian Aplikasi Dan Maklumat

Seksyen ini bertujuan menghalang capaian tidak sah ke atas maklumat yang terdapat di dalam sistem aplikasi. Kawalan capaian hendaklah:

- Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan;
- Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian *malicious* yang berupaya melangkaui kawalan sistem; dan
- Tidak berkompromi dengan sebarang sistem yang berkongsi sumber.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

- (a) Menghadkan capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna selaras dengan peraturan Kerajaan Negeri Johor; dan
- (b) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem yang berklasifikasi tinggi.

10.7 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Seksyen ini bertujuan memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan
- (b) Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Pernyataan Dasar

Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat sedia ada atau sistem maklumat baru hendaklah menyatakan keperluan-keperluan kawalan keselamatan.

Objektif

Untuk memastikan aspek keselamatan dikenal pasti dan diambil kira dalam semua sistem maklumat dan/atau perkhidmatan termasuk system pengoperasian, infrastruktur, sistem aplikasi dan sistem perisian. Aspek keselamatan ini mesti dikenal pasti, dijustifikasikan, dipersetujui dan didokumentasikan sebelum sesuatu sistem maklumat direka bentuk dan dilaksanakan.

11.0 Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat

Tanggungjawab Setiausaha Kerajaan Negeri adalah untuk:

- (a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat;
- (b) Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu; dan
- (c) Memastikan sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat.

11.1 Keperluan Keselamatan Sistem Maklumat

Seksyen ini bertujuan menjelaskan keperluan untuk memastikan bahawa aspek keselamatan dikenal pasti, dipersetujui dan di dokumen pada setiap peringkat perolehan, pembangunan dan penyelenggaraan.

Perkara yang perlu dipatuhi adalah termasuk pernyataan keperluan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

11.2 Pemprosesan Aplikasi Dengan Tepat

Seksyen ini bertujuan memastikan kawalan keselamatan yang sesuai diolah dan diterapkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan;
- (b) Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan;
- (c) Mengenal pasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan
- (d) Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.

11.3 Kawalan Kriptografi

Seksyen ini bertujuan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat melalui teknik kriptografi.

Perkara yang perlu dipatuhi adalah termasuk membangun kawalan kegunaan dan melaksanakan suatu peraturan kawalan kriptografi dan pengurusan kunci yang digunakan untuk menyokong teknik kriptografi bagi melindungi maklumat.

11.4 Keselamatan Fail-fail Sistem

Seksyen ini bertujuan memastikan capaian ke atas fail-fail sistem dan kod sumber program adalah terkawal dan aktiviti-aktiviti sokongan dilaksanakan dalam kaedah yang selamat. Kawalan perlu diambil untuk mengelakkan pendedahan maklumat sensitif semasa proses pengujian dilaksanakan.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam sistem yang sedang beroperasi;
- (b) Melindung dan mengawal data-data ujian; dan
- (c) Menghadkan capaian ke atas kod sumber program.

11.5 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Seksyen ini bertujuan memastikan keselamatan perisian system aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.

Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
- (b) Mengkaji semula dan menguji aplikasi kritikal semasa melaksanakan perubahan ke atas sistem yang sedang beroperasi untuk memastikan tiada impak negatif ke atas keselamatan atau operasi agensi;
- (c) Menghalang sebarang peluang untuk membocorkan maklumat; dan
- (d) Mengawal selia dan memantau pembangunan perisian oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat.

11.6 Pengurusan Teknikal Kerentanan (Vulnerability)

Seksyen ini bertujuan memastikan pelaksanaan pengurusan teknikal kerentanan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pelaksanaan pengurusan teknikal kerentanan ini perlu juga dilaksanakan ke atas sistem pengoperasian dan system aplikasi yang digunakan.

Perkara yang perlu dipatuhi adalah termasuk memperoleh maklumat teknikal kerentanan yang tepat pada masanya ke atas system maklumat yang digunakan, menilai tahap pendedahan agensi terhadap kerentanan tersebut dan mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Pernyataan Dasar

Insiden pelanggaran keselamatan hendaklah dilaporkan dengan sertamerta mengikut peraturan atau prosedur yang ditetapkan.

Objektif

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan.

12.0 Pengurusan Pengendalian Insiden Keselamatan

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri untuk mengurus dan mengendalikan insiden keselamatan ICT termasuk perkara-perkara berikut :

- (a) Menguruskan tindakan ke atas insiden yang berlaku sehingga keadaan pulih;
- (b) Mengaktifkan *Business Resumption Plan* (BRP) jika perlu; dan
- (c) Menentukan sama ada sesuatu insiden perlu dilaporkan kepada agensi penguatkuasaan undang-undang / keselamatan.

12.1 Insiden Keselamatan

Seksyen ini bertujuan untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan. Sesuatu insiden boleh berlaku dalam pelbagai keadaan. Insiden yang ketara dan sering berlaku di masa kini termasuk:

- (a) Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (*probing*);
- (b) Serangan kod jahat (*malicious code*) seperti *virus, trojan horse, worms* dan sebagainya;
- (c) Gangguan yang disengajakan (*unwanted disruption*) atau halangan pemberian perkhidmatan (*denial of service*);
- (d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorised access*); dan
- (e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

12.2 Melaporkan Insiden

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada *Computer Emergency Response Team (CERT)* Kerajaan Negeri Johor atau / dan *Government Computer Emergency Response Team (GCERT)* MAMPU. Semua maklumat adalah SULIT, dengan itu tidak boleh didedahkan tanpa kebenaran.

12.3 Menentukan Keutamaan Tindakan Ke Atas Insiden

Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan keparahan sesuatu insiden. Secara amnya keutamaan akan ditentukan seperti berikut:

Keutamaan 1:

Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

Keutamaan 2 :

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Pernyataan Dasar

Keperluan-keperluan keselamatan maklumat bagi kesinambungan perkhidmatan agensi hendaklah diwujudkan, dibangunkan dan disenggarakan.

Objektif

Untuk menjamin operasi perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

13.0 Kesinambungan Perkhidmatan

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri untuk menjamin perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

13.1 Tanggungjawab Melaksanakan Penilaian Risiko Keselamatan ICT

Adalah menjadi tanggungjawab Setiausaha Kerajaan Negeri memastikan penilaian risiko keselamatan ICT dilaksanakan secara berkala terutama apabila berlaku perubahan ke atas persekitaran agensi dan seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

13.2 Skop Penilaian Risiko Keselamatan ICT

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat di agensi termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur

yang dikendalikan oleh agensi. 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.

13.3 Penentuan Tindakan Untuk Mengendalikan Risiko Keselamatan ICT

Setiap agensi Kerajaan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT masing-masing. Melalui proses-proses yang dilaksanakan untuk menilai risiko aset ICT Kerajaan, agensi dapat mengenal pasti risiko-risiko yang wujud dan seterusnya mengenal pasti tindakan yang sewajarnya untuk menghadapi kemungkinan berlakunya risiko berkenaan.

Untuk mengenal pasti tindakan yang wajar diambil bagi menghadapi kemungkinan risiko terjadi termasuklah seperti 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;
- (d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan; dan
- (e) Merujuk kepada dokumen-dokumen HILRA dan MyRAM yang telah dikeluarkan oleh MAMPU.

13.4 Pelan Kesenambungan Perkhidmatan

Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan

perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan agensi. Pelan ini mestilah diperakui oleh pengurusan jabatan dan perkara-perkara berikut perlu diberi perhatian:

- (a) Mengenalpasti dan mendokumentasi semua tanggungjawab dan prosedur kecemasan atau pemulihan;
- (b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
- (c) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan
- (d) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

PEMATUHAN

Pernyataan Dasar

Keperluan-keperluan perundangan, *statutory*, peraturan atau ikatan kontrak hendaklah dinyatakan, didokumenkan dan dikemas kini.

Objektif

Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

14.0 Pematuhan Keperluan Perundangan

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan.

14.1 Pematuhan Dasar

Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

14.2 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan termasuklah seperti berikut:

- (a) Keselamatan perlindungan secara am

- i. *Emergency (Essential Power) Act 1964;*
- ii. *Essential (Key Points) Regulations 1965;*
- iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982;
- iv. Arahan Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985;
- v. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985;
- vi. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan
- vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 – Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan.

(b) Keselamatan dokumen

- i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);*
- ii. Akta Rahsia Rasmi 1972;
- iii. Akta Arkib Negara 2003;
- iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;

- v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 – Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);
- vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;
- vii. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M (R)10308 / 3 / (45) Bertarikh 8 Mei 1987;
- viii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK (R)200 / 55 Klt . 7 (21) Bertarikh 21 Ogos 1999; dan
- ix. Pekeliling Am Bil. 1 Tahun 2007 – Pekeliling Arahan Keselamatan Terhadap Dokumen Geospatial Terperingkat.

(c) Keselamatan fizikal bangunan

- i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;
- ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;
- iii. *State Key Points*;
- iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 – Keselamatan Jabatan-jabatan Kerajaan;
- v. Surat Bil. KPKK / 308 / A (2) bertarikh 7 / 9 / 79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/Jabatan;

- vi. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan
 - vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.
- (d) Keselamatan individu
- i. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti;*
 - ii. *General Circular Memorandum;*
 - iii. *Instruction On Positive Vetting Procedure;*
 - iv. Surat Pekeliling Am Sulit Bil.1 / 1966 - Perkara Keselamatan Tentang Persidangan- Persidangan / Perjumpaan/Lawatan Sambil Belajar Antarabangsa;
 - v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;
 - vi. Surat Pekeliling Am Sulit Bil.1 / 1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara tabir Buluh dan Tabir besi;
 - vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 – Melaporkan Perjumpaan / Percakapan Di Antara Diplomat / Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan

- viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.
- (e) Keselamatan aset ICT
- i. Akta Tandatangan Digital 1997;
 - ii. Akta Jenayah Komputer 1997;
 - iii. Akta Hak Cipta (Pindaan) 1997;
 - iv. Akta Multimedia dan Telekomunikasi 1998;
 - v. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;
 - vi. Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi;
 - vii. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);
 - viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan;
 - ix. *Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;*
dan
 - x. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.

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

14.3 Pelanggaran Perundangan

Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaiian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972.